نموذج ترخيص

أنا الطالب : حسام محمد فهد المصالحة أمنح الجامعة الأردنية و/ أو من تفوضه ترخيصاً غير حصري دون مقابل بنشر و / أو استعمال و / أو استغلال و / أو ترجمة و / أو تصوير و / أو إعادة إنتاج بأي طريقة كانت سواء ورقية و / أو إلكترونية أو غير ذلك رسالة الماجستير / الدكتوراه المقدمة من قبلي وعنوانها.

واقع أمن المعلومات من وجهة نظر العاملين بدائرة المعلومات في مكتبات الجامعات الأردنية والصعوبات التي يواجهونها

وذلك لغايات البحث العلمي و / أو التبادل مع المؤسسات التعليمية والجامعات و / أو لأي غاية أخرى تراها الجامعة الأردنية مناسبة، وأمنح الجامعة الحق بالترخيص للغير بجميع أو بعض ما رخصته لها.

اسم الطالب: حسام محمد فهد المصالحة

التوقيع:

التاريخ: ١٦/٨/٢٠١٦م

واقع أمن المعلومات من وجهة نظر العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية والصعوبات التي يواجهونها

إعداد

حسام محمد فهد المصالحه

المشرف

الدكتورة نشروان طه

قدمت هذه الرسالة استكمالا لمتطلبات الحصول على درجة الماجستير في

علم المكتبات والمعلومات

كلية الدراسات العليا

الجامعة الأردنية

آب، 2016

قرار لجنـة المناقشـة

نوقشت هذه الرسـالة (واقـع أمـن المعلومـات مـن وجهـة نظر العاملين بدوائر المعلومـات فـي مكتبات الجامعات الأردنية والصعوبات التي يواجهونها) وأجيزت بتاريخ 1 / 8 / 2016م

أعضاء لجنـة المناقشـة	التوقيـــــــــع
الدكتورة نشروان ناصر طه، مشرفاً أستاذ مساعد ـ علم المكتبات والمعلومات	....
الدكتور رائد جميل سليمان، عضواً أستاذ مشارك ـ علم المكتبات والمعلومات	....
الدكتورة فاتن فتحي حمد، عضواً أستاذ مساعد ـ علم المكتبات والمعلومات	....
الدكتور مصطفى حمدي أحمد، عضواً أستاذ مشارك ـ علم المكتبات والمعلومات (جامعة الحسين بن طلال)	....

الإهداء

إلى من بلغ الرسالة وأدى الأمانة ونصح الأمة ....سيدنا محمد صلى الله عليه وسلم

إلى من رباني على صدق القول والأخلاق الكريمة والرغبة في المعرفة....... والدي العزيز

إلى بستان المحبة الذي لا حدود له إلى نبع الحنان الذي لا ينضب......... والدتي الحبيبة

إلى من هم أحب إلي من نفسي حبا ووفاءا وعرفانا وتقديرا .... اخواني الأعزاء

إلى ورود المحبة وينابيع الوفاء ....أخواتي العزيزات

إلى من ساندوني ووقفوا بجواري............. جميع أصدقائي وزملائي

لأنكم كنتم رمزا للعون والعطاء والوفاء تستحقون جميعا أن أهديكم هذا الجهد المتواضع عرفانا مني بالجميل

الباحث

شكر وتقدير

الشكر لله تعالى صاحب الفضل الكبير الذي أنعم علي بالتوفيق والهداية ثم سخر لي كل الأسباب لإنجاز هذا العمل.

ثم أشكر المشرفة د. نشروان طه على ما بذلته من جهد كبير في اشرافها ومساعدتها لي وتقديم النصح والإرشاد ولما منحته لي من وقت وجهد لإخراج هذا العمل بهذه الصورة، فكانت آراؤها السديدة، وتوجيهاتها البناءة، وخبرتها الواسعة، مصباحا منيرا لبحثي.

كما أشكر جميع أساتذتي بقسم علم المكتبات والمعلومات لما لهم من فضل بعد الله في الحرص على رفع المستوى العلمي لي ولجميع الطلبة.

ولا يفوتني أن أتوجه بجزيل الشكر إلى أعضاء لجنة مناقشة هذا البحث. الدكتور رائد جميل، والدكتورة فاتن حمد، والدكتور مصطفى الراوي، على تفضلهم بقبول المناقشة.

والله ولي التوفيق

الباحث

قائمة المحتويات

قائمة الجداول

واقع أمن المعلومات من وجهة نظر العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية والصعوبات التي يواجهونها

إعداد

حسام محمد فهد المصالحة

المشرف

الدكتورة نشروان طه

الملخص

هدفت هذه الدراسة إلى تعرف واقع أمن المعلومات من وجهة نظر العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية، وتقصي أهم الصعوبات التي تواجههم، ومعرفة أثر متغيرات (سنوات الخبرة، ونوع الجامعة، والمستوى الوظيفي، والتخصص) في واقع أمن المعلومات، وفي الصعوبات التي تواجههم، وتكون مجتمع الدراسة من جميع العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية الحكومية والخاصة للعام الجامعي 2015–2016 وعددهم 96 موظفا، استجاب منهم 84، أي ما نسبته (87.5%).

ولغرض تحقيق أهدف الدراسة جرى تطوير استبانة لتقدير واقع أمن المعلومات، الذي تم تقسيمه إلى خمسة محاور، وهي: أمن البنية التحتية، وسياسة أمن المعلومات، وحماية البيانات الإلكترونية، وإجراءات حماية أنظمة وشبكات الحاسوب، والتحكم بالوصول لنظم المعلومات. واشتملت الاستبانة أيضاً على الصعوبات التي تواجه العاملين بدوائر المعلومات.

أظهرت النتائج أن واقع أمن المعلومات في المكتبات الجامعية الأردنية كان متوسطا، وأن محوري إجراءات حماية أنظمة وشبكات الحاسوب، والتحكم بالوصول لنظم المعلومات حازت على مستوى مرتفع، أما باقي المحاور فكانت من المستوى المتوسط، وأشارت لنتائج أن قسم الصعوبات حاز على مستوى متوسط، وتبين أن أهم الصعوبات التي تواجه العاملين بدوائر المعلومات في المكتبات الجامعية هي نقص عدد الموظفين المتخصصين في أمن المعلومات.

كما بينت الدراسة وجود فروق ذات دلالة إحصائية عند مستوى($\alpha \leq 0.05$) في واقع أمن المعلومات تعزى لمتغيري المستوى الوظيفي والتخصص، وأظهرت النتائج عدم وجود فروق دالة إحصائياً تبعا لمتغيري سنوات الخبرة ونوع الجامعة، وتبين وجود فروق دالة إحصائياً في الصعوبات التي تواجههم تعزى لمتغير التخصص، في حين تبين عدم وجود مثل هذه الفروق تبعا لمتغيرات سنوات الخبرة، ونوع الجامعة، والمستوى الوظيفي.

الفصل الأول

مشكلة الدراسة وأهميتها

المقدمة

يشهد العالم اليوم نمواً سريعاً وملحوظاً في تكنولوجيا المعلومات والاتصالات، وأثرت التكنولوجيا على جميع جوانب الحياة، وأصبحت المعلومات العنصر الأهم في هذا العصر، حيث شكل هذا النمو السريع في التكنولوجيا نقلة معلوماتية كبيرة وأصبح الحصول على المعلومات والتعامل معها أمراً في غاية الأهمية.

لقد احتلت المعلومات في عالمنا المعاصر منزلة رفيعة لأنها أصبحت قابلة للمعالجة والتناقل بأسرع من أي وقت مضى وإلى أي مكان في العالم نتيجة للانفجار الحاصل في تطوير تقنيتين كانتا منفصلتين. إذ ارتبطت فاعلية الحاسوب في معالجة وخزن المعلومات بتقنية الاتصالات وشبكاتها المتطورة لتشكل شبكة هائلة لمعالجة البيانات وتناقل المعلومات في جميع أنحاء الأرض، وأدى هذا الاقتران بين تقنية الحاسوب وتقنية الاتصالات إلى تفجر ثورة المعلومات التي يقطف العالم ثمارها اليوم في جميع مجالات الحياة، وأصبح هذا الاقتران شرطاً ومعياراً لنمو المؤسسات وتطورها (السرحان والمشهداني، 2001).

فالعالم اليوم يشهد ثورة معلومات كبيرة، وأصبحت أجهزة الحاسوب تختزن كميات هائلة من المعلومات وبدأت المعلومات تتحول تدريجياً إن لم تتحول بالفعل إلى معلومات رقمية. ولم يقف التحول عند هذا الحد، إذ أصبحت أمهات الكتب المؤلفة منذ مئات السنين تعاد كتابتها رقمياً، ويتصفحها القارئ من أي مكان في العالم. وأصبحت غالبية المجتمعات المعاصرة تلمس وبشكل يومي فائدة الثورة المعلوماتية في المجالات المختلفة. ومع هذا الإقبال من الأفراد والمؤسسات على استخدام تقنيات وشبكات المعلومات في جميع نواحي الحياة، بل والاستثمارات الضخمة في ظل ثورة المعلومات، برزت مشكلة كبيرة ألا وهي أمن المعلومات. فالمستخدمون العاديون، والمؤسسات، والهيئات والمنظمات، جميعهم يريدون استخداماً آمناً وتبادلاً موثوقاً للمعلومات المتداولة بينهم. وأصبح أمن المعلومات هو الهاجس الأول في ظل نمو شبكات المعلومات والاعتماد الكبير على المعلومات الإلكترونية في تنفيذ الأعمال اليومية على اختلاف أشكالها. ومن جانب آخر فإن ازدياد قيمة المعلومات وأهميتها لدى الناس والمؤسسات، جعلها هدفاً جذاباً للهجوم عليها من قبل الهواة والمحترفين وضعاف النفوس والمعتدين على حد سواء (القحطاني، 2008).

المشاكل الأمنية التي تواجهها المؤسسات والأفراد هي مشاكل مستمرة، حيث يسعى القراصنة والمخربون إلى إيجاد وسائل وتقنيات جديدة من أجل استخدامها في إجراء عملياتهم التخريبية والتدميرية، فكلما ابتُكرت طريقة جديدة لصد أنواع معينة من الهجوم والتهديد قام هؤلاء القراصنة بابتكار طرق جديدة أكثر خطورة من التي قبلها. ولا تأتي المشاكل الأمنية من هؤلاء القراصنة فقط، بل في أوقات كثيرة تأتي أيضاً سرقة المعلومات والأسرار والتهديدات من داخل المؤسسة (الطيطي، 2010).

وفي الوقت الذي حققت فيه الشبكة العنكبوتية حلماً لم يكن متوقعاً من قبل، إلا أنها خلقت العديد من المشاكل لمجتمع المعلومات الرقمي، من حيث الخصوصية والحماية وحقوق الملكية الفكرية، وبعض التجاوزات، بما في ذلك السرقة والتجسس والتلاعب الإلكتروني، وذلك نظراً لضخامة هذه الشبكة العملاقة، وكونها شبكة حرّة بعيدة عن سيطرة دولة بعينها (السالم، 2009).

وتعدُّ المكتبات ومراكز المعلومات من أكثر المؤسسات حاجة إلى استخدام الحاسوب وشبكات المعلومات لرفع مستوى خدماتها المقدّمة إلى المستفيدين، ومع التطور الذي شهده العصر الحديث في تنظيم المؤسسات والمعاهد العلمية، فقد استلزم ذلك تطوراً موازياً في المكتبات ومراكز المعلومات لتواكب هذا التطور ولتفي حاجات المستفيدين. ومع بدء عصر المعلومات لم يعد مجدياً التعامل أو حتى الاستمرار في معالجة المعلومات بالطرق التقليدية، كما أن التطورات المتسارعة في تكنولوجيا المعلومات تفرض على المكتبات ومراكز المعلومات خياراً واحداً لا بديل عنه، هو تبني التقنيات الحديثة لتحافظ على مكانتها في علم المعلومات (يونس، 2003).

فالمكتبات تأثرت بهذه التطورات التكنولوجية الحديثة، حيث حرصت على التعامل مع المصادر الإلكترونية والنظم الآلية ومواكبة جميع التطورات. إلا أنه وفي ظل هذا التطور التكنولوجي الذي أصبحت فيه أشكال التهديد والمخاطر مختلفة عما كانت عليه من قبل، أصبحت المكتبات عامة والمكتبات الجامعية خاصة تواجه هذه المخاطر وتشكل لها هاجساً كبيراً لا بدَ من مواجهته والوقوف عنده. ولأهميّة هذا الموضوع، وقلة الدراسات المتوفرة حوله، جاءت هذه الدراسة التي تهدف إلى تعرّف واقع أمن المعلومات من وجهة نظر العاملين في دوائر المعلومات في مكتبات الجامعات الأردنية والصعوبات التي يواجهونها.

مشكلة الدراسة وأسئلتها:

إن الدور الذي تلعبه مؤسسات المعلومات وبالأخص المكتبات الجامعية في خدمة مجتمع المستفيدين في ظل التطورات التكنولوجية الحديثة التي أحدثتها البيئة الرقمية منذ نشأتها، أدى إلى

ظهور أجهزة وتبني أساليب جديدة في خدمات المكتبات الجامعية ساعدت على تسهيل وتبادل المعلومات لضمان بقاء المكتبات الجامعية في الريادة من أجل خدمة مجتمع المستفيدين.

والمكتبات الجامعية الأردنية شأنها كغيرها من مؤسسات المعلومات، لا تستطيع أن تنعزل عن هذه التطورات التكنولوجية؛ فقد استحدثت أنظمة وأساليب جديدة من أجل خدمة البحث العلمي وخدمة مجتمع المستفيدين منها، إلا أن هذه التطورات أدت إلى زيادة احتمالية انتهاك وتسرب المعلومات وتعرضها لخطر التغيير والتزوير، والتعدي على مقتنياتها الرقمية سواء بشكل متعمد أو غير متعمد.

وتقوم دوائر المعلومات في المكتبات الجامعية بأعمال البرمجة التي تحتاجها هذه المكتبات والإشراف على قواعد البيانات والدوريات الإلكترونية ، وعمل الإجراءات اللازمة للمحافظة على مقتنياتها مثل الباركود، والإشراف على الأنظمة مثل: أنظمة المكتبات المتكاملة، وإتاحة الرسائل الجامعية إلكترونياً. وللتعرف على واقع أمن المعلومات في المكتبات الجامعية الأردنية في ظل هذه التطورات التكنولوجية وللحاجة الماسة للبحث في هذا الموضوع ؛ جاءت هذه الدراسة للتعرف على واقع أمن المعلومات من وجهة نظر العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية والصعوبات التي يواجهونها.

وتحديداً تحاول الدراسة الإجابة عن الأسئلة التالية:

1. ما واقع أمن المعلومات من وجهة نظر العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية؟
2. ما الصعوبات التي تواجه العاملين في دوائر المعلومات في التصدي للانتهاكات الإلكترونية في مكتبات الجامعات الأردنية؟
3. هل هناك فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين المتوسطات الحسابية لتقديرات العاملين بدوائر المعلومات في المكتبات الجامعية الأردنية لواقع أمن المعلومات تعزى إلى متغيرات سنوات الخبرة، ونوع الجامعة، والمسمى الوظيفي، والتخصص؟
4. هل هناك فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين المتوسطات الحسابية لتقديرات العاملين بدوائر المعلومات في المكتبات الجامعية الأردنية للصعوبات التي تواجه العاملين بدوائر المعلومات في التصدي للانتهاكات الإلكترونية في مكتبات الجامعات الأردنية تعزى إلى سنوات الخبرة، ونوع الجامعة، والمسمى الوظيفي، والتخصص؟

أهداف الدراسة :

تحاول الدراسة تحقيق جملة من الأهداف، لعل أهمها:

1. تعرّف واقع أمن المعلومات في مكتبات الجامعات الأردنية.
2. تعرّف الصعوبات التي تواجه العاملين بدوائر المعلومات في التصدي للانتهاكات الإلكترونية في مكتبات الجامعات الأردنية.
3. التعرّف على ما إذا كان هناك فروق ذات دلالة إحصائية بين المتوسطات الحسابية لتقديرات العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية لواقع أمن المعلومات تعزى إلى متغيرات: سنوات الخبرة، ونوع الجامعة، والمستوى الوظيفي، والتخصص.
4. التعرّف على ما إذا كان هناك فروق ذات دلالة إحصائية بين المتوسطات الحسابية لتقديرات العاملين بدوائر المعلومات للصعوبات التي تواجه العاملين بدوائر المعلومات في التصدي للانتهاكات الإلكترونية في مكتبات الجامعات الأردنية تعزى إلى متغيرات: سنوات الخبرة، ونوع الجامعة، والمستوى الوظيفي، والتخصص.

أهمية الدراسة:

تكتسب الدراسة أهميتها من أهمية الموضوع الذي ستتناوله وهو واقع أمن المعلومات من وجهة نظر العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية والصعوبات التي يواجهونها، ومن أهمية أمن المعلومات في الحفاظ على المعلومات وحمايتها من الأخطار والأضرار المختلفة، وتنبع أهميتها أيضاً من قلة بل ندرة الدراسات العلمية حول الموضوع، ويمكن أن يستفيد كل من الأطراف التالية من نتائج الدراسة:

1. إدارة المكتبات الجامعية، فمن خلال اطلاعهم على نتائج هذه الدراسة يمكنهم التعرف على مستوى أمن المعلومات، مما يساعدهم على تطوير إستراتيجيات جديدة لحل المشكلات ذات العلاقة.
2. العاملون بالمكتبات الجامعية؛ إذ إن اطلاعهم على نتائج هذه الدراسة سيزيد من وعيهم بأهمية أمن المعلومات.
3. الباحثون في مجال علم المكتبات والمعلومات، وخاصة الذين يريدون إجراء دراسات مشابهة.
4. أقسام المكتبات والمعلومات في الجامعات الأردنيّة، إذ إن هذه الدراسة ستحفزهم على طرح مواد متخصصة في أمن المعلومات.

مصطلحات الدراسة:

فيما يلي تعريف بالمصطلحات المهمة الواردة في الدراسة:

أمن المعلومات (Information Security)

الإجراءات والتدابير التي تستخدم لحماية المصادر البيانية (أجهزة وبرمجيات وبيانات وأفراد) من التجاوزات والتداخلات غير المشروعة التي تقع عن طريق الصدفة أو عمداً عن طريق التسلل أو نتيجة للإجراءات الخاطئة أو غير الوافية المستخدمة من إدارة هذه المصادر (الجواد والفتال، 2008).

وإجرائياً: يعرف أمن المعلومات بأنه مجموعة الإجراءات والتدابير التي تستخدمها مكتبات الجامعات الأردنية لحماية مصادرها الإلكترونية، والتي ستقاس من خلال الدرجة الكلية لاستجابات أفراد الدراسة على فقرات أداة الدراسة.

المكتبة الجامعيّة: (University library)

هي المكتبة أو مجموعة المكتبات التي تنشؤها وتمولها وتديرها الجامعات، وذلك من أجل تقديم الخدمات المكتبية والمعلوماتية المختلفة لمجتمع الجامعة بجميع شرائحه (عليان وأبو زيد، 2002).

وإجرائياً: يقصد بها جميع المكتبات الجامعية الأردنية الحكومية والخاصة، وتتمثل في: مكتبة الجامعة الأردنية، ومكتبة جامعة اليرموك، ومكتبة جامعة مؤتة، ومكتبة جامعة العلوم والتكنولوجيا، ومكتبة جامعة آل البيت، ومكتبة الجامعة الهاشمية، ومكتبة جامعة البلقاء التطبيقية، ومكتبة جامعة الحسين، ومكتبة جامعة الطفيلة، ومكتبة الجامعة الألمانية الأردنية، ومكتبة جامعة عمان الأهلية، ومكتبة جامعة الشرق الأوسط،، ومكتبة جامعة جدارا، مكتبة جامعة فيلادلفيا، ومكتبة جامعة الإسراء، ومكتبة جامعة البترا، ومكتبة جامعة الزيتونة، ومكتبة جامعة الزرقاء، ومكتبة جامعة إربد الأهلية، ومكتبة جامعة جرش، ومكتبة جامعة الأميرة سمية للتكنولوجيا، ومكتبة الجامعة الأمريكية، ومكتبة جامعة عجلون الوطنية، ومكتبة جامعة العلوم التطبيقية.

أمن المكتبات:

أمن وسلامة المكتبات ونظمها وشبكاتها ومحتوياتها والعاملين بها بشكل مباشر وغير مباشر (السريحي، 2002).

دوائر المعلومات في المكتبات الجامعية:

يقصد يها إجرائيا الدوائر والأقسام التي تقوم بأعمال البرمجة التي تحتاجها المكتبات الجامعية والإشراف على قواعد البيانات والدوريات الإلكترونية ، وعمل الإجراءات اللازمة للمحافظة على مقتنياتها، مثل الباركود، والإشراف على الأنظمة، مثل: نظام الأفق، وإتاحة الرسائل الجامعية إلكترونياً.

العاملون بدوائر المعلومات:

يقصد بهم إجرائيا: مديرو ورؤساء الأقسام والشعب، والموظفون في دوائر المعلومات، وهم الذين أجابوا على أداة الدراسة.

المصادر الإلكترونية:

هي الأعمال التي تسجل وتنظم وتخزن وتسترجع بشكل إلكتروني باستخدام الحاسوب وملحقاته، مثل: الدوريات ، والرسائل الجامعية، و المكتبات المحوسبة (عليان، 2010).

وإجرائياً: مصادر المعلومات الإلكترونية التي تتوافر في مكتبات الجامعات الأردنية موضوع الدراسة.

الصعوبات التي يواجهونها العاملين بدوائر المعلومات:

يقصد بها إجرائيا مجموعة التحديات والصعوبات التي تواجه العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية من وجهة نظرهم، والتي ستقاس درجة إحساسهم بها من خلال الإجابة على فقرات الجزء المتعلق بالصعوبات في أداة الدراسة.

حدود الدراسة ومحدداتها:

تتحدد هذه الدراسة بما يلي:

الحدود المكانية: تحددت هذه الدراسة في المكتبات الجامعية الحكومية والخاصة في الأردن.

الحدود الزمانية: تم تطبيق الدراسة في العام الجامعي 2015-2016.

الحدود البشرية: اقتصرت هذه الدراسة على العاملين في دوائر المعلومات في جميع المكتبات الجامعية الأردنية الحكومية والخاصة.

محددات الدراسة: تحددت نتائج الدراسة بمجتمع الدراسة وأداة الدراسة من حيث دلالات صدقها وثباتها، والمعالجة الإحصائية.

الفصل الثاني

الإطار النظري والدراسات السابقة

أولاً: الإطار النظري:

المقـــدمة:

إن المعلومات في هذا العصر بناء تحتي ترتكز عليه النظم السياسية والاجتماعية والإدارية والتربوية، فهي ثروة وذات قيمة عالية، واكتسابها يتطلب مهارة كبيرة، الأمر الذي جعلها عرضة للتهديد والاختراق، وعلى الرغم من كلفة المعلومات المتمثلة في قيمتها وندرتها إلا أن تقنية المعلومات وأوعيتها وفرت المعلومة بشكل كبير، وأصبحت جرائم المعلومات ونظمها تتزايد بشكل كبير، والتحقيق فيها والحكم عليها عملية معقدة (البداينة،2002).

لقد أدى التطور في شبكات المعلومات الذي كان متزامنا مع التطور في أجهزة الحاسوب وأنظمة المعلومات إلى ازدياد في مشاكل أمن المعلومات من حيث المحافظة على سرية وتكاملية وخصوصية البيانات والتأثير على الخدمة التي تقدمها الكثير من الأنظمة مما يشكل خطراً كبيراً على المنشآت الحكومية والخاصة، ومع دخول الإنترنت في حياتنا بشكل كبير تمكن الكثير من المستخدمين من الحصول على أدوات تساعدهم اختراق أنظمة الحاسوب، وبما أنه ليس هناك نظام أمني مطلق ستزداد المشاكل مع ازدياد الاعتماد على الحاسوب وشبكة الإنترنت (رمضان، 2009).

إن من أهم أهداف تقنية المعلومات إتاحة استخدام هذه التقنيات لكل العالم بشكل سهل وغير معقد، ومن أجل الحصول على ثقة المستخدمين فإن هناك العديد من نقاط الضعف في هذه التقنيات. كذلك فإن جميع الخدمات في السابق كانت معتمدة على طبيعتها الأساسية ومن ثم كان الاعتقاد بأن الشبكة محمية بشكل ممتاز، ولم تؤخذ بعين الاعتبار المشاكل الأمنية التي من الممكن أن تظهر، لذلك كان من السهل اعتراض هذه البيانات وقراءتها والقيام بكل العمليات غير المصرح بها، مثل تغييرها وحذفها وغير ذلك. أما في عصر الإنترنت فقد تم أخذ موضوع الأمن بشكل أكثر جدية ولكن بقيت الكثير من الفجوات الأمنية موجودة (الطيطي، 2010).

وعند دراسة أمن منظومة الحاسوب لا بد من أخذ العديد من المشاكل بعين الاعتبار، ومن أهمها توفير الحماية اللازمة والضرورية للبيانات المخزنة فيها للاستفادة منها بشكل متكامل ودقيق، فوضع الحماية اللازمة والمتكاملة للمعلومات ضمن منظومة الحاسوب يستوجب تطبيق مجموعة من الإجراءات الأمنية إضافة إلى تطبيق سياسات معينة ضمن هذا المجال، كما أنها تحتاج إلى كادر بشري واعٍ لمهمته وجهد ووقت، بالإضافة إلى موارد مالية وفنية مناسبة لوضع نظام الحماية موضع التنفيذ. وهناك مجموعة من إجراءات الحماية تطبق على الكيان المادي

للحواسيب، وأخرى تطبق على برمجياتها، كذلك لا بد من توفير حماية مناسبة لخطوط الاتصالات بين عقد شبكة الحاسوب، إضافة الى الجهد البشري الذي يكون ممثلا ومتابعا لهذه الإجراءات علما أن طبيعة الحماية المستخدمة تعتمد بشكل أساسي على أهمية المعلومات المستخدمة وعلى الإمكانيات المادية والفنية لمركز المعلومات وكفاءة الأشخاص المحتمل انتهاكهم إجراءات الحماية هذه، (السرحان والمشهداني، 2001).

يشكل الأمن في أية مؤسسة قلقا عاما لدى جميع الموظفين، فمشكلة الأمن لا تعكر صفو المديرين العاملين فحسب، بل تتعداهم لتصل المستخدمين النهائيين في كل مستوى ضمن المؤسسة، والخطوة الأولى لتحقيق أمن أية مؤسسة، هي أن يعلم جميع الموظفين ضمن هذه المؤسسة أن مسؤولية الأمن هي مسؤولية جماعية، وإن كل حماية فردية وكل جهد مبذول لتحقيق الأمن هو خطوة على طريق تحقيق الأمن الكلي للمؤسسة. وللوصول إلى المستوى المطلوب من أمن المعلومات لا بد من معرفة وضعه القائم حاليا؛ لذلك يتم إجراء الدراسات والاستقصاءات، والدول النامية تعاني نقصا كبيرا في هذا المجال (الغثبر والصبيح، 2012).

والمكتبات اليوم تعتمد وبشكل متزايد على تكنولوجيا المعلومات، والعديد من المكتبات قد توقف بطاقات الفهرسة وغيرها من الوسائل التقليدية لصالح الإصدارات الإلكترونية، فكثير من مصادر المعلومات التي كانت محصورة داخل أبنية المكتبات هي الآن متاحة الكترونيا ويمكن الحصول عليها من أي مكان من خلال البحث عنها في قواعد البيانات وغيرها (Newby,2002)

وترى بامفلح (2003) أن المكتبات توازن بين إتاحتها لمصادر المعلومات وبين أساليب الحماية المتبعة، آخذة بعين الاعتبار أن تشديد الإجراءات الأمنية سيؤدي إلى قلة الاستخدام أحيانا. وفي عصر المعلومات الذي اختلفت فيه أساليب التهديد ظهرت في المكتبات أساليب جديدة للحماية مختلفة أيضا، فهناك حاجة للحفاظ على أمن المعلومات بدرجة أكبر في ظل شبكات المعلومات بسبب الخطر الذي تواجهه المعلومات عند إتاحتها من خلال هذه الشبكات. وأكد السالم (2008) على ضرورة الاهتمام بالعنصر البشري وتطويره في مجال المكتبات والمعلومات لأنه يمثل ثروة لخدمة التنمية الوطنية في كافة المجالات.

مفهوم أمن المعلومات

أمن المعلومات من القضايا الساخنة باستمرار وخصوصاً في السنوات الأخيرة بعد التطور الذي حدث في أجهزة الحاسوب ووسائل الاتصال، ويعرف أمن المعلومات على أنه " حماية وتأمين كافة الموارد المستخدمة في معالجة المعلومات، حيث يتم تأمين المنشأة نفسها والأفراد العاملين فيها وأجهزة الحاسبات المستخدمة فيها ووسائط المعلومات، حيث يتم تأمين المنشأة، ويتم ذلك عن طريق اتباع إجراءات ووسائل حماية عديدة تضمن في النهاية سلامة المعلومات وهي الكنز الثمين الذي يجب على المنشأة الحفاظ عليه" (داود، 2004).

ويعني أيضاً حماية المعلومات والأنظمة من خلال إجراءات وأدوات تتخذها المؤسسات لمنع الدخول غير المصرح به (Kritzinger and Smith, 2008).

ويعرف أمن المعلومات بأنه حماية المعلومات وعناصرها الهامة من وصول الأشخاص أو الجهات غير المصرح لها، ومن السرقة أو العبث بها عمدا أو سهوا، ومن الضرر بكافة أشكاله سواءً من أشخاص أو برامج، والأخطاء العفوية، والكوارث كالحريق والفيضانات وغيرها (القحطاني، 2008).

ومن ناحية إدارية يعرفه إيلوف وإيلوف Eloof and Eloof (2003) على أنه التخطيط والتنفيذ للممارسات والإجراءات الإدارية التي تهدف للحفاظ على أمن المعلومات.

عناصر أمن المعلومات

إن حماية المعلومات من كافة جوانبها أمر في غاية الأهمية في هذا العصر الذي تعددت فيه وسائل الاتصال وازداد فيها اعتماد الأشخاص والمؤسسات على المعلومات المخزنة إلكترونيا في أعمالهم اليومية. وفيما يلي أهم عناصر أمن المعلومات (القحطاني، 2008):

1. التحقق من الهوية (Authentication): وتعني التأكد من هوية الشخص أنه هو المعني وليس شخصا آخر، بمعنى آخر هو التأكد من أن مستخدم النظام هو من ادعى أنه ذلك المستخدم، فيجب التأكد من هوية المرسل وأيضا من هوية المستخدم لضمان أن المعلومة في وجهتها الصحيحة. كما يطلق على التحقق من الهوية "المصادقة" التي تضمن أن الطرفين هما فعلا الأشخاص المعنيون. ويمكن التحقق من الهوية باستخدام معيار أو معيارين أو ثلاثة وذلك حسب درجة قوة التحقق المطلوبة، وذلك كما يلي:

- استخدام معيار واحد: هو معيار "ماذا تعرف" مثل استخدام كلمات المرور أو أرقام التعريف الشخصية Personal Identification Number (PIN). يتمثل هذا المعيار بطلب إدخال معلومة لا يعرفها إلا الشخص المعني فقط.

- استخدام معيارين: وذلك من خلال استخدام معيار "ماذا تعرف" بالإضافة إلى معيار "ماذا تملك"، وتتمثل هذه الطريقة بطلب إدخال معلومة لا يعرفها إلا الشخص المعني ومعلومة أخرى لا يملكها إلا نفس الشخص أيضا، ومن الأمثلة بطاقة الصرف الآلي حيث يتم التحقق من خلال رقم البطاقة التي لا يملكها إلا الشخص المعني ثم إدخال الرقم السري الذي لا يعرفه إلا هو ولا يمكن أن يغني أحدهما عن الآخر.
- استخدام ثلاثة معايير: تتمثل هذه الطريقة بطلب معلومة أو أكثر من الخصائص الشخصية بالإضافة إلى المعيارين السابقين. فمثلا بصمات الأصابع أو العين وأبعاد راحة اليد وغيرها. وتعتبر هذه الطريقة أكثر تعقيدا من الطرق السابقة وتحتاج إلى أجهزة وبرامج إضافية.

2. التحكم بالوصول (Access Control): يقصد به التحكم بالوصول إلى الموارد المتاحة ويأتي هذا العنصر بعد عنصر التحقق من الهوية، ليتم التحكم باستخدام الشخص لموارد محددة من الشبكة وليس جميع الموارد، ولذلك يتم تحديد قائمة التحكم بالوصول للموارد الهامة في الشبكة، حيث تحدد هذه القائمة الأشخاص المصرح لهم فقط باستخدامها. وذلك يشمل منع الاستخدام غير المرخص به لأي معلومة، وكذلك تحديد الصلاحيات للأشخاص المصرح لهم بالوصول للمعلومات تحت شروط معينة، فمن الممكن أن يكون لدى أشخاص صلاحية القراءة فقط وأشخاص لهم صلاحية الطباعة وآخرون بإمكانهم الحذف وغير ذلك. ومن الجدير بالذكر أن تقييد المعلومات بقوائم طويلة ومعقدة قد يؤدي إلى عدم القدرة إلى الوصول للمعلومات في الأوقات المناسبة، وبالمقابل فإن تركها مفتوحة لأي شخص قد يسبب خللا أمنيا واستنزافا للموارد بشكل كبير، فلا بد من الموازنة من خلال السماح بوصول معقول مع أخذ الاعتبار لجميع التهديدات المحتملة، وعلى سبيل المثال فإن حجب قاعدة بيانات بشكل كامل يسبب عدم الحصول على المعلومة، وفتحها بالكامل يسبب خللا أمنيا، ففي هذه الحالة يفضل حجب بعض الحقول الهامة في قاعدة البيانات وترك بعضها الآخر مفتوحا.
3. السرية (Confientialitity): وتعني المحافظة على المعلومات من الاطلاع عليها من قبل الأشخاص غير المخولين بذلك. أي لا يجب أن يطلع على المعلومة إلا المرسل أو المرسل إليه، وإذا استطاع أحد الإطلاع عليها فيجب أن تكون غير مفهومة له، وتعتمد السرية على عدة طرق أهمها التشفير من خلال خوارزميات رياضية معقدة. فتشمل السرية حماية البيانات أثناء نقلها من المتطفلين أو من يحاول كسر سريتها، وتتراوح طرق توفير السرية بين حجب المعلومة يدويا وتسليمها للأشخاص المصرح لهم فقط إلى طرق التشفير الحديثة المعتمدة على الخوارزميات المعقدة التي يصعب فكها.

4. سلامة وتكامل المعلومات (Data Integrity): التأكد من محتوى المعلومات أنه سليم ولم يتم عليه التعديل أو الحذف أو الإضافة. ولأنها معلومة إلكترونية فمن الممكن أن تتعرض للتغيير مع أنها مشفرة، لذلك فإن هذا الأمر مهم لضمان الثقة في المعلومة . وبمعنى آخر تعني سلامة وتكامل المعلومة بأنه تم تلقي الرسالة كما أرسلت بالفعل، فهذا العنصر يهتم بكشف عدم سلامة المعلومة أكثر منه عملية منع التعديل للمعلومة أو تصحيح ذلك التعديل والسبب في ذلك أن المعلومة تصبح غير آمنة بمجرد التعديل غير المشروع عليها حتى وإن تم تصحيح ذلك التعديل. وتبرز هنا أهمية كشف إعادة توجيه الرسالة وكشف إعادة تركيبها لأنه في هذه الحالة تصل الرسالة كاملة ولكنها غير سليمة. ولا تقف قدرة كشف التعديل عند التعديل الذي ينتج عنه تشويه واضح للمعلومة بل يتعداه إلى كشف أي تعديل حتى لو بقيت المعلومة بعده وكأنها لم تتغير.

5. عدم الإنكار (Non-Repudiation): منع أي شخص أو جهة من إنكار العمليات التي قام بها، وضبطها في أوقات وتواريخ معينة عن طريق إلحاق بصمة الوقت والتاريخ.

6. توفر المعلومة: أن تكون المعلومة متاحة وقت الطلب من أي شخص أو جهة مصرح لها الحصول عليها. ولا بد من الموازنة بين توفر المعلومة وحمايتها؛ فإذا كان الحصول على المعلومة لأي شخص ومن أي مكان وبأي طريقة اتصال سيكون هناك صعوبات أمنية.

ويرى كانكانهالي وآخرون Kankanhalli et al. (2003) أن ممارسة المهام الأمنية في المنظمة يمكن تصنيفها إلى عوامل خارجية تشمل (الأمن المادي والإداري والأفراد) وداخلية تتعلق بالأجهزة والبرمجيات، وللمحافظة عليها لا بد من إجراءات رادعة لثني الناس عن السلوكات الإجرامية وذلك من خلال تشريع العقوبات، وإجراءات وقائية من خلال إعاقة الوصول غير المصرح به واحتياطات مادية والتعاون بين المنظمات وغيرها. وذكر براكر ووالس Braker and Wallace (2007) أن ضوابط أمن المعلومات تقسم إلى ثلاث فئات :

1. ضوابط فنية: تشمل برامج مكافحة الفيروسات وكشف التسلل وتقنيات التشفير.
2. ضوابط التشغيلية: وتشمل السيطرة المادية على الدخول والحماية من الاخطار.
3. ضوابط إدارية: وتشمل استخدام سياسات لأمن المعلومات وتدريب الموظفين والتخطيط.

طبيعة وتحديات المشكلة الأمنية

أشار داود (2000) إلى أن التطور التقني أثر على أمن المعلومات وزادها حدة، ففي هذا العصر أصبحت الأجهزة -سواء كانت شخصية أو متوسطة أو كبيرة- في تطور مستمر وسرعات تشغيل البرامج فيها تصل إلى آفاق كبيرة ما كنا نظن أنها ستصل إليها، وطاقات تخزين

المعلومات على الوسائط المختلفة تزداد كل يوم في ظل تنافس كبير بين شركات الحاسب، وسرعة الوصول إلى المعلومات في تطور مستمر بالإضافة إلى تعاظم قدرات ذاكرة الحاسب. ويتواكب مع هذا التطور تطور مواز في البرمجيات، فالشركات تتسابق في إنتاج برمجيات أكثر سهولة للمستخدمين وأكثر كفاءة في المعالجة. فهذا التطور كان له آثار ملحوظة على أمن المعلومات سواء سلبا أو إيجابا، ولكن بصفة عامة فإن هذا التطور في أغلب الأحيان أسرع من أن تتم ملاحقته من قبل خبراء أمن المعلومات لتغطية الثغرات الناتجة عن النظم الجديدة الأكثر تعقيدا. ويمكن القول أن مجالات التطور التقني التي أبرزت مشكلة أمن المعلومات تتمثل بما يلي:

1. تشغيل البرامج أصبح ممكنا في بيئات بعيدة: فقد سمح الاتجاه إلى نظم التشغيل الموزعة بتشغيل مواقع بعيدة جغرافيا بكفاءة عالية، فمن الممكن تشغيل البرنامج في بيئة عمل أخرى أو مركز حاسب آخر وترسل برنامجك لينفذ على حاسب بعيد، فهذا الأمر خلق مصادر تهديد جديد فالبرامج التي تستضيفها دون أن تدري لا تضمن أنها أمينة.

2. أصبحت قواعد البيانات العالمية في متناول اليد: فقد أصبح الوصول إلى قواعد البيانات العالمية والحصول منها على معلومات في أي مكان بالعالم أمرا سهلا، وهذه التسهيلات يصاحبها احتمالات انتهاكات، فقد لا يكون من السهل السيطرة على من يدخلون إلى قواعد البيانت الخاصة بالمنشأة أو التحكم فيما يصلون إليه من معلومات.

3. لم يعد المتخصص هو القادر الوحيد: فمن خلال لغات البرمجة الحديثة سهلة الاستخدام التي لا يحتاج استخدامها خبرة كبيرة أصبح وضع قوة المعالجة في أيدي أعداد كبيرة من المستخدمين، أي أن الشخص العادي يستطيع البرمجة والبحث في قواعد البيانات، وهذا ربما يتيح له الاطلاع على معلومات محظورة إضافة إلى إمكانية تعديل هذه المعلومات وتدميرها.

4. صعوبة السيطرة على تسرب المعلومات في زمن المؤتمرات عن بعد: لقد أصبح من الممكن الآن عقد هذه المؤتمرات من خلال الشبكات الرقمية للخدمات المتكاملة Integrated Services Digital Networks وإمكانياتها الكبيرة. أصبح من الممكن نقل الصوت والصور والرسوم وأفلام الفيديو بسهولة عبر هذه الشبكات، وهذا جعل الرقابة على خروج المعلومات ودخولها -سواء للمؤسسات أو حتى الدول- أمرا في غاية الصعوبة.

إن القدرة على تقييم المخاطر هي الخطوة الأولى لإدارة الخطر حيث يتم تقييم أثر التهديدات التي من شأنها أن تحدث خللا في المنظومة الأمنية، ويتم ذلك من خلال وضع إستراتيجيات وقائية للحد أو التقليل من هذه المخاطر (Summer,2009). تتطلب دراسة مشكلة أمن المعلومات تسليط الضوء على مجموعة من الحقائق التي تحكم بيئة المعلومات، وأهمها: (الجواد والفتال، 2008)

1. الاتجاه المتزايد نحو تخزين المعلومات المهمة داخل أوعية مركزية عرفت بقواعد البيانات والذي أدى إلى زيادة المخاطر التي تتعرض لها المصادر البيانية، ولا يقلل من هذه المخاطر توزيعها على مواقع جغرافية مختلفة ما دام أن هذه الأنظمة مرتبطة من خلال شبكات الاتصال.
2. أصبح هناك سهولة في التقاط مصادر البيانات عن طريق استخدام منافذ اتصال زهيدة التكلفة مع ارتفاع طاقة وقدرة هذه الأجهزة على البث. وبهذا تحولت النظم الالكترونية من مجرد أداة مساعدة إلى أسلوب للإدارة لا يمكن الاستغناء عنه.
3. هناك نقص في الوعي بأمن المعلومات بسبب حداثة ظاهرة الانتهاك نوعاً ما إلى جانب اتجاه الكثير من المؤسسات إلى التكتم على الأخبار التي تتصل بعمليات الاختراق، إما نتيجة الخوف من توجيه النقد أو الخوف من تكرار المحاولات من جانب أشخاص قد يسعون لاستغلال نقطة الضعف.
4. يتم التغاضي عن كثير من المشاكل والانتهاكات أو التقليل من شأنها إذا كان تأثيرها على العمليات اليومية العادية ضئيلا ومحدودا، وكثير من المؤسسات لا تدرك قيمة مصادرها البيانية ودرجة تأثيرها على سياساتها وأهدافها.
5. العديد من إجراءات الحماية المتبعة، سواء ما يتعلق منها بإجراءات التدقيق وتعريف الهوية أو إجراءات الحماية من الوصول غير المخول أو إجراءات التشفير تحتاج إلى تطوير.
6. في كثير من الأحيان يصعب اكتشاف أو تتبع التغيرات التي تطرأ على المصادر البيانية بسبب تشعب وتعقد النظم وبالتالي فإنه من الصعب إقامة الأدلة على القائمين بهذه الأعمال.
7. نقص وعجز التشريعات القانونية في هذا المجال، فمعظم هذه القوانين لا تفرق بين القيمة الحقيقية للمعلومات والقيمة المادية للأوساط التي استخلصت منها المعلومات.
8. هناك بعض الظواهر فيما يتعلق بحوادث الاحتيال باستخدام الحاسبة مثيرة للاهتمام، وهي أن الأشخاص الذين ينفذون عملية احتيال كبرى بهذا الأسلوب ولا يتم اكتشافهم بسرعة يصبحون أبطالا استطاعوا بذكائهم أن يهزموا النظام الأمني المتبع حتى في نظر القضاة أحيانا.

ويرى عرب (2005) أن الاعتداءات في ظل بيئة المعلومات تطال مكونات تقنية في أربعة مواطن:

1. الأجهزة: وهي كافة الأدوات والمعدات المادية التي تتكون منها النظم.
2. البرامج: وهي أوامر مرتبة وفق نظام معين لإنجاز الأعمال.

3. المعطيات: وهي كافة البيانات والمعلومات المستخرجة بعد معالجتها، وقد تكون طور الإدخال والإخراج أو التخزين أو التبادل بين النظم عبر الشبكات، وقد تخزن على وسائط تخزين أو داخل النظم.
4. الاتصالات: وتشمل الشبكات الداخلية والخارجية، وتتيح فرصة اختراق النظم من خلالها، وهي أيضا محل اعتداء ومن مواطن الخطر الحقيقي.

التحديات التي تواجه أمن المعلومات

أشار رمضان (2009) إلى أن التحديات الست التي تواجه أمن المعلومات تتمثل بما يلي:

1. متطلبات التجارة الالكترونية : ان شبكة الإنترنت اصبحت مركزا هاما للقيام بأعمال التجارة الإلكترونية، وقد أصبح وجود مواقع للشركات على الإنترنت ضرورة وليس من الكماليات، فهذا المصدر وفر العديد من الأساليب للمؤسسات لتسويق منتجاتها، وأصبح في مقدور المؤسسات الصغيرة ذات المواردالمحدودة التواصل مع عملائها طوال الوقت، وعبر موقعها على الشبكة بسبب توسع استخدام الإنترنت. ومع تطور هذه الخدمات ظهرت مصاعب جديدة يجب التغلب عليها للاستمرار في تقديم الخدمات والمنتجات عبر الإنترنت.
2. ازدياد الهجمات على أمن المعلومات: مع ازدياد هجمات الفيروسات على مواقع الشركات تحولت من حالات مزعجة الى ضارة، وكانت في السابق تصيب أجهزة محدودة، أما اليوم فإن آثارها تنعكس على غالبية الأجهزة المرتبطة بالشبكة العنكبوتية، مما يلحق خسائر مادية كبيرة.
3. منتجات أمن المعلومات غير الناضجة: بعض الشركات المنتجة لأنظمة أمن المعلومات تحتفظ بجزء معين ومحدود من متطلبات أمن المعلومات، مما ينتج عنه صعوبة في تكامل تلك الحلول الجزئية التي تعمل مع بعضها بعضا.
4. النقص الكبير في موظفي أمن المعلومات: هناك صعوبة في إيجاد الأشخاص الأكفياء المتخصصين في أمن المعلومات، ومما زاد صعوبة توفر المختصين في أمن المعلومات عدم نضج منتجات حماية المعلومات وقلة المواصفات القياسية أو انعدامها، وتعدد المنتجات الفردية التي تخدم جانبا واحدا من جوانب أمن المعلومات، لذلك أصبح تدريب الفنيين في أمن المعلومات أمرا صعبا ومكلفا.
5. التشريعات الحكومية: فمن خلال زيادة الاعتماد على الشبكة العنكبوتية، وزيادة حوادث أمن المعلومات، أخذت الحكومات تعمل تشريعات إضافية لتنظيم بيئة الأنظمة المعلوماتية. وبما أنه يمكنك الدخول إلى الإنترنت والتعامل عن طريقه مع كل العالم، فليس من المهم تطبيق القوانين والتشريعات ذات العلاقة بأمن المعلومات في البلد الذي يوجد به الشركة، بل يجب أن تطبق

كافة التشريعات والقوانين الملزمة في البلدان التي يوجد بها عملاء لتلك الشركات. وأصبح لزاما على الشركات أن تطبق تشريعات بلدها وكافة بلدان العالم التي يوجد بها عملاء لها.

6. القوى العاملة المتحركة والحوسبة اللاسلكية: أثرت أجهزة الحاسب المتنقلة على نمط الحياة اليومية، فالاتصال اللاسلكي زاد من خلال الهاتف الجوال وتصفح الإنترنت والبريد الإلكتروني عبر الأجهزة المحمولة المتصلة لا سلكيا.

إن إدارة الأمن الفعالة ثلاثة عوامل رئيسية

1. ضرورة التزام الإدارة العليا ودعم أمن المعلومات.
2. تنفيذ الضوابط المناسبة للحد أو التقليل من المخاطر والتهديدات.
3. التواصل مع المستخدمين وتوعيتهم في كل ما يخص أمن المعلومات من خلال التدريب (Fulfurd and Doherty,2003).

ويؤكد الهادي (2006) أن كثيرا من التحديات تحد من الأداء السليم لنظم المعلومات ومنها: المشكلات الفنية والتطورات التكنولوجية المتسارعة والضعف البشري وعدم مواءمة المؤسسات للتغيرات المتلاحقة وغيرها، وتنبع هذه المخاطر من أفعال مقصودة وغير مقصودة ومن مصادر داخلية أو خارجية، وربما تكون مفاجئة، أو أحداثا ثانوية تؤثر على كفاءة العمل أو إبطائه.

ويشير الطائي والكيلاني (2015) أن هناك تهديدات طبيعية تشمل الكوارث والفيضانات والزلازل وغيرها، وتتأثر في هذه التهديدات أنظمة المعلومات والأجهزة والمعدات، وغالبا ما يكون تأثيرها شاملا وكبيرا لأنها خارجة عن الإرادة البشرية. وهناك أيضا تهديدات بشرية وتصنف إلى:

1. المهاجمون من الداخل: وهم الأفراد الذين ينتمون للمؤسسة لكنهم يقومون بأعمال تخالف الجهود الرامية إلى حماية المعلومات الخاصة بتلك الجهة، وممكن أن يكون ذلك بقصد أو غير قصد. ومن أسباب الهجوم من الداخل حالة عدم الرضا التي يشعر بها الموظف، وإثبات الشخص مهاراته الفنية وقدرته على تنفيذ هجوم إلكتروني، أو تحقيق مكاسب من خلال سرقة المعلومات السرية.
2. المهاجمون من الخارج: ويطلق عليهم قراصنة (Hackers)، ومن دوافعهم للقيام بمهاجمة الأنظمة أهداف سياسية أو دينية، أو تحقيق مكاسب مالية، أو التجسس على المؤسسة.

التهديدات الرقمية

ليس بالضرورة أن يكون الخرق الأمني قد حصل حقيقة ليتم اعتباره تهديدا وإن حقيقة خرق الأمن قد حصل يعني بأن هناك مسببات لحدوثه لا بد من العمل على تحصينها من أجل عدم تكرار هذا الخرق الأمني، إن عملية التهديد هي أن هناك احتمالا لعملية خرق أمني للمؤسسة أو الأفراد. وفيما يلي بعض التهديدات الأمنية التي تواجه البيئة الرقمية (الطيطي، 2010):

1. التطفل: وهو نوع من كشف سرية المعلومات حيث يتم اعتراض المعلومات التي يتم نقلها بين الأطراف بطرق غير شرعية.
2. التغيير أو التعديل: وهي عملية غير مصرح لها يتم فيها القيام بتغيير أو تعديل للمعلومات بهدف الخداع، حيث يتم قبول معلومات غير صحيحة على أنها صحيحة.
3. انتحال الشخصية أو التنكر: هذا النوع يضلل الشخص على التصديق بأن الكائن المزور هو الكائن الحقيقي، وهو نوع من الخداع وأخذ السلطة للوصول إلى المعلومات بطرق غير مشروعة.
4. التأخير: منع أو حجب الخدمة مؤقتاً بدون حق شرعي.

ويرى وذيام (2004) Withiam أن تهديدات أمن المعلومات تشمل الأخطاء البشرية والتعدي على الملكية الفكرية والوصول غير المصرح به للبيانات والأعمال المتعمدة لتخريب أو تدمير نظم المعلومات وسرقتها والهجمات على البرمجيات مثل الفيروسات والديدان والحرمان من الخدمة والتهديدات الطبيعية مثل انقطاع الكهرباء والأعطال الفنية مثل تعطل الأجهزة والتقادم التكنولوجي.

وأشار الصاحب (2013) لعدد من الضوابط للإجراءات المضادة للمخاطر:

1. ضوابط التوجيه: التي عادة ما تكون إدارية ووضع السياسات والمطالبة بالعمل بمقتضاها.
2. الضوابط الوقائية: التي تحمي النظام من نقاط الضعف، وتحد من الهجوم وآثاره وتحتاج لرقابة مستمرة لعناصر النظام.
3. ضوابط الكشف: تؤدي لكشف الهجمات.
4. ضوابط الإنعاش التي تكون غالبا مرتبطة مع استمرارية العمل.

الأمن المادي للمعلومات

إن حماية المعلومات لا تقتصر على الحماية التقنية فقط، وإنما يجب حمايتها أيضا من الأخطار الخارجية أيضا كالسرقة والحريق والماء والتخريب وعبث المعتدين والفضوليين. فالحماية المادية لها دور هام في منظومة أمن المعلومات، فمهما كلفت برمجيات الحماية والتجهيزات الفنية من مبالغ كبيرة فلن تستطيع أن تؤدي دورها إذا تمت سرقتها أو العبث بها،

فالمنشآت الحكومية والخاصة تهتم اهتماما كبيرا في الحماية المادية لمواقعها بشكل عام ولأنظمة ومصادر المعلومات بشكل خاص (القحطاني، 2008).

متطلبات الحماية المادية

يرى القحطاني (2008) أن هناك جملة من المتطلبات التي يجب توفيرها في المنشآت وهي:

1. يكون الأثاث حسب ما تستدعي الحاجة فقط، وتجهيز المنشأة بمواد غير قابلة أو بطيئة للاشتعال.
2. تجهيز المكان بنظام تكييف جيد، وهناك أنظمة تكييف تمدد وتوزع الهواء بمراكز البيانات خاصة لمثل هذه المواقع.
3. أن يكون هناك نظام خاص بمكافحة الحريق.
4. تجهيز نظام جيد لمكافحة تسريب المياه.
5. حصر المساحة اللازم تبريدها، واستخدام الأرضيات المرتفعة لتسهيل التمديدات تحتها.
6. استخدام كبائن لوضع أجهزة التخزين والأجهزة الرئيسية ومغذيات الطاقة بداخلها مع تزويدها بنظام أقفال إلكترونية للتحكم بها.
7. تخزين أقراص وأشرطة النسخ الاحتياطي في خزانات خاصة فولاذية مضادة للرطوبة والحريق .
8. مراقبة وضبط درجة الحرارة ومستوى الرطوبة في المنشأة.
9. استخدام أقفال آلية للأبواب الهامة تعمل ببطاقات إلكترونية أو بأرقام سرية.

منظومة الطاقة الكهربائية

من خلال التلاعب بمستويات الطاقة المجهزة للمنشآت يمكن اعتبار معدات وأجهزة الطاقة الكهربائية وسيلة لعمليات التخريب، مما يلحق الضرر بمنظومة الحاسوب بشكل عام. ولذلك يفضل أن يكون هناك مناطق مقفلة يمكن مراقبتها بسهولة ومنع الاقتراب منها يوضع بها المحولات وخطوط التغذية وأجهزة التغذية الكهربائية المستمرة والبطاريات الملحقة بها ومعدات توليد الطاقة في الحالات الطارئة وغيرها (الجواد والفتال، 2008).

وأشار داود (2000) إلى ضرورة استخدام مصدر يضمن الإمداد بالطاقة بشكل مستمر واختبار وصيانة البطاريات الخاصة به باستمرار، وعند انقطاع مصدر تغذية الطاقة الكهربائية الرئيسي لا بد من العمل على توفير الطاقة الكهربائية للمبنى باستعمال مولدات احتياطية لتوليد الكهرباء، واختبار كفاءة هذه المولدات بشكل دوري، وتأمينها بمصادر الوقود اللازمة لها،

ويفضل توفر مفتاح تحويل يدوي للكهرباء مع المفتاح الآلي في وحدة السيطرة لاستعماله في حال أي عطل أو خلل بالمفتاح الآلي.

الوقاية من الحريق

هناك أمثلة كثيرة على حوادث الحريق في مؤسسات المعلومات التي أدت إلى أضرار كثيرة فمثلا الحريق الذي حدث في إحدى دوائر الولايات المتحدة عام 1973 نجم عنه خسائر مادية قدرت ب(6) مليارات دولار أمريكي بسبب أكثر من (7) آلاف شريط ممغنط وتم تدمير أجهزة ومعدات عديدة إثر هذا الحريق. كذلك الحريق الذي حدث بإحدى جامعات بريطانيا عام 1985 نتج عنه أضرار كبيرة في المعدات والبناء، إلا أنه وبسبب الإجراءات التي كانت تتخذها في حفظ النسخ الاحتياطية للملفات والبرامج وحفظها خارج المبنى، تم حماية الكثير من البحوث والدراسات المخزنة فيها من التلف لذا يجب اعداد نظام متكامل للوقاية من الحريق أو التقليل من الخسائر المحتملة عند حدوثه وذلك لتحقيق الحماية المطلوبة من الأضرار المحتملة للحرائق، متضمنا عدة إجراءات كما يلي (السرحان والمشهداني، 2001):

- يكون الموقع مصمما بشكل يقلل من امكانية انتقال الحريق من الخارج الى الداخل، وتكون أجهزة التكييف مصصمة أيضا بشكل لا يجعلها سببا في انتقال الحريق، وتخزين المواد القابلة للاشتعال بشكل يقلل من قابليتها لذلك.
- توفر أجهزة ومعدات اكتشاف وإطفاء الحرائق في جميع أنحاء المبنى وفحصها بشكل دوري، والتأكد من عمل صافرات الإنذار وفحصها دوريا لأنها تساعد في التنبيه للخروج من المبنى، وتوفر مكبر الصوت لاستخدامه عند الحاجة، ووجود أقنعة صالحة لمن يحتاجها عند حدوث الحريق.
- توعية العاملين من مخاطر الحريق من خلال المحاضرات والدورات وتعليق التعليمات على الجدران، ومنع التدخين داخل المبنى واتخاذ إجراءات صارمة لمحاسبة المخالفين، وتسجيل أسماء العاملين عند خروجهم وذلك للتأكد من خلو المبنى من أي شخص للتقليل من الخسائر البشرية.

أمن الأجهزة

هناك إجراءات يتم اتباعها للحفاظ على سلامة الأجهزة، وتتمثل بما يلي (داود، 2000):

1. خضوع دخول الأجهزة وخروجها لموافقة مسؤول أمن نظام المعلومات.
2. تأمين الخدمات التي قد يؤدي توقفها تلفا بالأجهزة مثل الطاقة الكهربائية وتكييف الهواء.

3. وجود إجراءات معروفة ومعلنة تتبع عند الطوارئ لفصل التيار الكهربائي والتدريب عليها من آن لآخر.
4. مرافقة مسؤولي الصيانة من خارج المؤسسة خلال عملهم.
5. وضع إجراءات يتم استخدامها عند إخراج الأجهزة للصيانة خارج المبنى أو إعادتها.

أمن الأفراد

إن حرية دخول الأفراد إلى المؤسسات حسب طبيعتها، فيكون دخولهم في المؤسسات الحكومية والمالية فوق المتوسط، في حين أن المؤسسات الجامعية تكون حرية الدخول فيها مباحة أكثر، إذ لا توجد آلية شاملة لمراقبة دخول الأفراد، وهناك ثلاثة معايير تتحكم في دخول الأفراد: هي الشيء المحمول والشيئ المعلوم والخصائص المادية، فالشيء المعلوم هو بطاقات الموظفين التي تحوي صورة شخصية ومفاتيح مرمزة مغناطيسيا، وهذه غير مكلفة وسهلة في حملها، لكنها معرضة للفقدان أو السرقة ويمكن استعارتها وتبادلها بين الأشخاص. أما الشيء المعلوم فيقصد به أرقام البطاقة أو كلمة السر أو الأرقام السرية للأقفال، وتتميز بانخفاض التكلفة وسهولة اكتشاف الخطأ ولكنها تعاب بأنه من الممكن استعارة وتبادل كلمات السر (الجواد والفتال، 2008). ويرى جيان وآخرون jain et al. (2006) أنه من الممكن التعرف على الخصائص الشخصية عن طريق أجهزة مطابقة شكل الوجوه وشكل اليد وبصمات الأصابع وتهدف إلى ايجاد أسلوب يقلل من دخول الأفراد غير المصرح لهم .

ونشر الوعي الأمني بين الأفراد يجب أن يكون من أكبر المخاوف اليوم، فمهما بلغت وسائل وتقنيات أمن المعلومات من تطور فإنها قد تفشل بسبب خطأ بشري صغير، ولا تزال درجة الوعي الأمني لمستخدمي التكنولوجيا ضعيفة بسبب إهمالهم لهذا الجانب، وتتراوح أبرز المخاطر ذات الصلة على شبكة الإنترنت من سرقة هويات المستخدمين وكلمات المرور واقتحام الخصوصية وانتهاكات حقوق الملكية. لذلك من الضروري أن تقوم المنظمات على تدريب المستخدمين ليكونوا أكثر وعيا بالمخاطر الأمنية التي من الممكن أن يتعرضوا لها (Show et al.,2009).

إن بعض المؤسسات تعترف أن موظفيها غالبا ما يكونون الحلقة الأضعف في مجال أمن المعلومات نتيجة لقلة الوعي وعدم امتثالهم للمعايير الأمنية. فالمؤسسات التي ترغب في الاستفادة من رأس المال البشري لا بد لها من تطوير سلوكهم وامتثالهم للسياسات والقواعد الأمنية وتوعيتهم بها وتحفبزهم، فالوسائل التكنولوجية وحدها لا تكفي لحماية مصادر المعلومات

والتكنولوجيا إذا لم نهتم بالعنصر البشري في المؤسسة، لذلك يجب الاهتمام بالعنصر البشري (Bulgurcu et al.,2010).

ويرى داود (2000) أن هناك إجراءات يجب اتباعها للمحافظة على أمن الأفراد:

1. تنظيم ومتابعة تسجيل دخول وخروج الموظفين وتنقلهم في المبنى.
2. وجود سجل للزوار وتنظيم دخولهم ومرافقتهم داخل المبنى.
3. متابعة سجل عمليات المستفيدين وخاصة الذين لديهم صلاحيات عالية لاستخدام البيانات.
4. اشتراط تحديث كلمات السر.
5. تحديد الإجراءات المتبعة في حالة الاستقالة أو إنهاء الخدمة وتغيير كلمة السر الخاصة به.
6. اختيار الموظفين بعناية وإجراء التحريات اللازمة خصوصا بالنسبة للأجانب.
7. عدم حصول الموظف حديث التعيين على صلاحيات عالية لاستخدام النظام.
8. وجود قائمة أو نظام آلي لدى مسؤول أمن نظام المعلومات تضم جميع الأشخاص المصرح لهم باستخدام النظام ودرجات صلاحياتهم.
9. تدريب مستخدمي النظام بشكل مناسب، واشتراط عدم إفشاء المعلومات الحساسة أو إجراءات الأمن والرقابة.

وأشار السالم (2010) إلى ضرورة تطوير المهارات التقنية للعاملين في مؤسسات المعلومات، فقد أصبحت في الوقت الراهن بيئة المعلومات معقدة ويجب على العاملين في هذا المجال مواجهة الواقع من خلال التطوير المهني والتعلم الذاتي، فنظام المعلومات شديد التأثر بالتغيرات الخارجية والتطورات في مجال الاتصالات والشبكات التي تفتح الباب أمام عالم غير مستقر وأفق غير متناه، ويضع هذا مهمة الاستعداد على العاملين في هذا القطاع والتعامل معه بعقلية منفتحة من خلال البرامج التدريبية والمشاركة في المناسبات العلمية مثل المؤتمرات والندوات وغيرها، وأيضا من خلال برامج الابتعاث المحلي والخارجي وقاعات النقاش المفتوحة وغير ذلك من النشاطات التي تنمي مهاراتهم.

سياسة أمن المعلومات

هي تحديد كيفية أداء الأعمال ذات العلاقة بأمن المعلومات عن طريق الخطوات المكتوبة، وتبين هذه السياسة كيفية معالجة أي حدث يخص أمن المعلومات وكيفية استخدام التقنية الموجودة لمعالجة ذلك، وتعتبر هذه السياسة من أهم الأمور للتخطيط لأمن المعلومات، ومنها يمكن أن ننطلق لتطبيق الخطة على أرض الواقع (القحطاني، 2008).

وتهدف سياسة أمن المعلومات إلى تعريف المستخدمين والإداريين بالواجبات والالتزامات المطلوبة لحماية النظم والشبكات وحماية المعلومات بكافة أشكالها وجميع مراحلها، وتهدف أيضا إلى تحديد الطريقة التي يتم من خلالها تنفيذ الواجبات المحددة على كل من له علاقة بالمعلومات ونظمها وتحديد المسؤوليات عند حدوث أخطار، وتوضيح الاجراءات التي يجب اتباعها لتجاوز أي خطر أو تهديد والتعامل مع الجهات المناط بها القيام بذلك (عرب، 2005).

إن دعم وتأييد الإدارة العليا أمر مهم عند إنشاء سياسة أمن المعلومات، فذلك يضمن اهتمام الموظفين بها وتنفيذها، وعدم دعم الادارة العليا سيؤدي إلى فشل هذه السياسة ومن طرق كسب تأييد الادارة العليا توضيح القيمة الحقيقية للمعلومات وإطلاعهم على المقالات والكتب ذات العلاقة بالموضوع والتعرف على بعض الأحداث للمنشآت التي تضررت بسبب عدم تطبيق سياسة لأمن المعلومات. ومع أن هناك الكثير من الباحثين الذين يؤكدون أن الخطوة الأساسية لخطط الأمن هي وجود سياسة مناسبة، إلا أن أكثر من 60% من المنشآت ليس لديها سياسة أمنية أو أنها قديمة وغير محدثة (الكردي، 2011).

وتجدر الإشارة إلى أن هناك جانبا كبيرا من أمن المعلومات، هو في الحقيقة جانب إداري وإجرائي يتمثل بالسياسة الأمنية، فالسياسات الأمنية إجراءات إدارية تطبق على أرض الواقع من خلال الأنظمة والبرامج المتاحة، ومن الأمثلة على ذلك أن تنص السياسة الأمنية في حال عدم إدخال كلمة المرور بشكل صحيح لثلاث مرات متتالية فإن حساب المستخدم يعطل ولا يفعل مرة أخرى إلا عن طريق مدير الشبكة، ويمكن القول أن السياسة الأمنية هي بمثابة قانون يحدد التعريفات والإجراءات المقبولة على كافة المستويات الإدارية، ولا بد لها أن تكون واضحة ودقيقة وتحدد أيضا الإجراءات الواجب اتخاذها في حالات الصواب وفي الحالات الخاطئة. ولا بد من أن تكون هناك سياسة عامة للمؤسسة توضح إجراءات منح الصلاحيات للموظف، مثل كلمات المرور واستخدام شبكة الإنترنت وخطة مواجهة الكوارث وغيرها، ويمكن إعداد سياسة أمنية تشمل جميع أعمال المنظمة، كما يمكن أن تقسم إلى سياسة أمنية لكل جزء وذلك حسب طبيعة هذه المؤسسات (القحطاني، 2008).

خصائص وثيقة السياسة الأمنية

إن سياسة أمن المعلومات لها أهمية خاصة لأنها توفر الخطط للأمن الشامل وتساعد على تنفيذ ممارسات آمنة في المؤسسات، وتهدف إلى توفير التوجيه الإداري والدعم لأمن المعلومات ومطابقة متطلبات العمل مع القوانين واللوائح التنظيمية (Knapp et al.,2009).إن السياسة

الأمنية يسترشد بها كل من المستفيد والإدارة العليا كي يسترشد بها الفريقان عند اتخاذ القرارات، ولا بد أن تتسم بعدة صفات كما يلي: (داود، 2004)

1. الوضوح الكامل: حيث تكون مفهومة وواضحة، وجميع القيود والإجراءات التي تحتويها تكون مبررة ومقنعة، حتى يتبعها الجميع، والاستمرار باتباعها حتى عند رحيل واضعيها.
2. تحديد مسؤوليات كل شخص: من خلال وضوح المسؤوليات والواجبات الملقاة على كل موظف ومسؤول وكل مستفيد، فلا تكون متركزة على عاتق مسؤولي الأمن فتعطي بذلك أن دور المستفيد هو دور هامشي، وبنفس الوقت لا تكون متركزة على المستفيد فتكون عدائية وغير عادلة.
3. استخدام لغة واضحة بسيطة: لا بد ان تكون اللغة المكتوبة بها السياسة الأمنية واضحة سهلة الفهم والتطبيق، فالمستفيدون ليسوا كلهم من خبراء أمن المعلومات.
4. فرض السياسة (السلطة): فإذا اكتفت المؤسسة بكتابة هذه السياسة ولم يتم تنفيذها فلن تستفيد شيئا، لذلك يجب أن تتضمن تحديد من لديهم صلاحية حرمان المستفيد من الخدمة عند المخالفة، أو إيقاف بعض الخدمات التي تؤثر على الشبكة أو أمن المعلومات.
5. إتاحة المجال للحالات الخاصة: تحديد أسلوب تعديل السياسة الأمنية للسماح بالاستثناءات عندما تظهر حالات خاصة تستدعي ذلك، فلا توجد سياسة أمنية تغطي كل حالات الحاضر والمستقبل.
6. إتاحة المجال للمراجعة: يجب مراجعة السياسة الأمنية وتعديلها عبر الزمن عندما تظهر مستجدات أو تقنيات أو ظروف جديدة، فمثلا من الممكن أن يزداد عدد العاملين أو تزداد سرعة الخطوط المتاحة أو تدخل المؤسسة مجالا جديدا لم تكن داخلة فيه من قبل كالتجارة الإلكترونية مثلا.

ما يجب أن تحتويه السياسة الأمنية

يرى القحطاني (2008) أن السياسة الأمنية يجب أن تحتوي على البنود التالية:

- الإجراءات التي يجب اتخاذها بما يخص أمن المعلومات وموارد المنشأة عند تعيين موظف جديد أو إنهاء خدمات موظف سابق.
- تقسيم المستفيدين إلى مجموعات وتحديد صلاحيات كل مجموعة.
- لضمان أمن وحسابات المستخدمين لا بد من وضع الشروط والقيود اللازمة لكلمات المرور.
- تحديد متى يتم إيقاف حساب المستخدم وتعطيل حسابه لفترة معينة أو منعه من دخول شبكة المنشأة أو إعادة تفعيل حسابه.
- تحديد من الذين يسمح لهم بتركيب أجهزة أو برامج إضافية على أجهزتهم.

- إجراءات أمن المعلومات الواجب تطبيقها على الشبكة بشكل عام وعلى كل جهاز على حدة، كتفعيل التحديث التلقائي لأنظمة التشغيل وقفل منافذ الاتصال وتحديد الأوقات المناسبة لذلك.
- إجراءات حماية الشبكة من الفيروسات.
- آلية النسخ الاحتياطي وتحديد مسؤوليات وصلاحيات عمل ذلك.

ويضيف سرما وكبشلات Sirma and Kipchillat (2014) أن السياسة الأمنية تتضمن طرق التحكم بالوصول واستمرارية الأعمال ومواجهة الكوارث وتصنيف البيانات واسترجاعها وأمن تظم المعلومات واستخدام الإنترنت.

وأشار داود (2004) إلى عدة نقاط يجب ألا تحتويها سياسة أمن المعلومات، منها:

- يجب عدم ظهور التفاصيل الفنية لكيفية حماية الأصول في السياسة الأمنية أو لكيفية الحماية من الفيروسات أو أسلوب عمل جدار الحماية أو غير ذلك من التفاصيل التي تؤدي معرفتها إلى تسهيل مهمة المهاجمين لشبكة المؤسسة
- يجب ألا تعكس السياسة الأمنية للمؤسسة سياسة مؤسسة أخرى أو تقليدا لجهة أخرى. فلكل مؤسسة مخاطر معينة تود مكافحتها ولها قيود مختلفة، وطبيعة المستفيدين مختلفة، والقدرات المالية مختلفة، بل يجب أن تختلف سياسة المؤسسة نفسها عبر الزمن وعند تغير احتياجاتها.
- يجب ألا تتعرض السياسة لأمور لا علاقة لها بصميم أمن المعلومات، فقد تدخل بعض الأمور في باب الآداب العامة أو سوء استخدام مكان العمل. فيجب أن نركز على ما يؤثر على أمن المعلومات فقط. فمثلا لا يعنينا إن كان الموظف يستخدم جهازه في ألعاب الكمبيوتر أو المحادثة، بل نهتم بكيفية اتصاله بالآخرين وهل هذا الاتصال مؤمن أم لا .

الاختراق

إن الهجوم الإلكتروني أصبح سهلا ما دام أن معظم أجهزة الحاسب مرتبطة بالإنترنت والشبكات الخاصة، فالبيئة الالكترونية المتنامية تسهل عملية الهجوم وتصعب من عملية رصدها، وزيادة الأجهزة المرتبطة بالشبكات تعني زيادة الأهداف الجاذبة للهجوم أو الاختراق. فالاختراق هو القدرة على الوصول لهدف معين بالطرق غير المشروعة من خلال الثغرات الموجودة في نظام الحماية الخاص بالهدف (القحطاني، 2008).

ويقسم علوة (2011) الاختراق من حيث الطريقة المستخدمة إلى:

1. اختراق المزودات والأجهزة الرئيسية للشركات أو المؤسسات أو الجهات المختلفة، وذلك عن طريق اختراق الجدران النارية (FireWall)، وتم ذلك من خلال المحاكاة (Spoonfing) وهي عملية انتحال شخصية للدخول إلى النظام، حيث إن حزم Internet Protocol (IP) (عناوين

الإنترنت) تحتوي على عناوين للمرسل والمرسل إليه، وهذه العناوين ينظر إليها كعناوين مقبولة وسارية المفعول من قبل البرامج وأجهزة الشبكة، فتعطى حزم ال IP شكلا تبدو فيه وكأنها قادمة من جهاز معين، بينما هي في الحقيقة ليست قادمة منه، ويتم ذلك من خلال طريقة تعرف بمسارات المصدر (Source Routing)، فالنظام إذا وثق بهوية مصدر الحزمة فإنه يكون قد حوكي أو خدع.

2. اختراق الأجهزة الشخصية والعبث بالمعلومات التي تحتويها، وهي طريقة شائعة بسبب جهل بعض أصحاب هذه الأجهزة من جانب وسهولة تعلم برامج الاختراق من جانب آخر.
3. التعرض للبيانات أثناء انتقالها والتعرف على شيفرتها إن كانت مشفرة.

وقد قسم القحطاني (2008) المهاجمين إلى هواة أو محترفين، وإن العديد من الناس قد ينظرون للمهاجم نظرة تقليدية على أن هذا المهاجم هو شخص في عمر المراهقة ولديه وقت فراغ كبير، وقد تم الترويج لهذا النوع النمطي من المخترقين من خلال الأفلام والأشخاص الحقيقيين الذين ألقي القبض عليهم بهذا الخصوص.

مجالات الاختراق

ذكر الطائي والكيلاني (2015) عدة مجالات لاختراق أمن المعلومات، منها:

1. الملفات الورقية: فلا تزال هذه الملفات تستحوذ على النسبة الكبرى من الملفات المستخدمة رغم استخدام النظم الحاسوبية، وأهم الفرص المتاحة في هذا المجال:

- عدم تصنيف المواد بشكل يمكن من خلاله معرفة مدى السرية التي تنطوي عليها ومن ثم حفظ هذه الملفات في مواقع أمينة.
- الاستعمال الزائد لأجهزة النسخ وبشكل أكبر من المقرر، أو نسيان النسخة الأصلية في الجهاز أو محاولة بعض الأفراد نسخ وثائق حساسة والاحتفاظ بها لأنفسهم.
- رمي النسخ التالفة التي تحتوي على معلومات هامة دون النظر لهذا الجانب.
- فشل إدارة المنظمة في التعامل مع المعلومات التي تنشرها تلك المنظمة والتي قد تضم معلومات حساسة.
- عدم التعامل بشكل صحيح مع المعلومات التي انتفت الحاجة إليها، مثل رميها بسلة النفايات مما قد يعرضها للاستغلال من قبل الأفراد الذين يتعاملون بها أو قد يتم البحث عنها بشكل قانوني باعتبارها نفايات مهملة ولا حاجة لها من قبل المؤسسة.

2. أجهزة الفاكس: فقد قدمت هذه الأجهزة مزايا متعددة للمنظمات مثل السرعة والسهولة وانخفاض التكلفة، ومع ذلك فإنها تتيح الفرص لاختراق أمن المعلومات، أهمها:

- وضعها في أماكن عامة دون قيود تمنع الوصول إليها قد يعرضها للاختراق، فمثلا يستطيع المخترق أن يضع لاقطة ناقلة أو انتظار ما يسجله خاصة في حالة ضعف الرقابة على هذه الأجهزة.
- الاستفادة من الخطوط الهاتفية التي يمكن أخذ خط منها بسهولة وبالتالي الوصول غير المرخص به للمعلومات.

3. التجسس وانتحال الشخصية: ويضم هذا المجال عدة فرص متنوعة، وتتصف بشكل عام بكونها توفر الاطمئنان لد الأفراد العاملين بالمنظمة، وذلك لجعلهم يتحدثون عن المنظمة ومعلوماتها بكل سهولة، ومن الأمثلة على هذه الأساليب:

- الجولات السياحية الاستطلاعية التي يقوم بها هؤلاء الأشخاص.
- ادعاء الرغبة في التوظيف وطلب التعيين.
- الادعاء بأنهم باحثون أو محللون أو استشاريون أو طلبة، وذلك للحصول على معلومات عن المنظمة وأنشطتها والأفراد العاملين فيها.
- الادعاء بأنهم من كوادر الخدمات في المنظمة مثل عمال الصيانة.

4. الملفات الإلكترونية: وهناك فرص كثيرة يتيحها هذا المجال، منها:

- إساءة استخدام كلمة السر مثل اشراك الأفراد الآخرين فيها والاستمرار مدة طويلة دون تغييرها.
- ترك المحطات الطرفية (Terminals) مفتوحة إذ يفتح المجال للوصول إلى المعلومات بكل سهولة .
- ترك حافظات الأقراص مفتوحة يتيح الفرصة للاطلاع عليها أو سرقتها أو العبث بها.

وهناك آثار متعددة للاختراق، يذكر علوة (2011) عددا منها:

1. تغيير الصفحة الرئيسية لموقع الويب كما حدث لموقع فلسطيني مختص بالقدس حيث غير بعض الاسرائيليين الصور الخاصة بالقدس إلى صور تتعلق بالديانة اليهودية بعد عملية الاختراق.

2. السطو بقصد الكسب المادي أو الحصول على خدمات مادية أو أي معلومات ذات مكاسب مادية.

3. الحصول غير المشروع على كلمات السر التي يستخدمها الشخص للحصول على خدمات مثل الدخول إلى الإنترنت، حيث يلاحظ الضحية أن ساعاته تنتهي دون أن يستخدمها، وغير ذلك.

الفيروسات

إن الفيروسات بدأت بالظهور عام 1988 على شكل برامج لها قدرة على إفساد العملية الصحيحة في الأجهزة، واستطاعت أن تلحق أضرارا طفيفة، وسرعة انتشارها قليلة، وعندما تطورت الأجهزة والبرمجيات وأصبحت شبكات الحاسب أداة أساسية للحياة اليومية بدأ تأثيرها يتضاعف، وأصبح لهذه الفيروسات رموز أكثر تعقيدا، وهي قادرة على تطوير نفسها عدة مرات وقادرة على الحصول على البيانات الشخصية لمستخدمي الشبكة مثل كلمات السر والحسابات المصرفية وغيرها مما تسبب في أضرار جسيمة للأفراد والمؤسسات (Roberto and Araujo,2009)

الفيروس برنامج يهدف إلى إلحاق الضرر بنظام الحاسوب، وتكون له قدرة على ربط نفسه بالبرامج الأخرى وتكرار نفسه، مما يتيح له الفرصة للانتشار داخل الحاسوب في أكثر من مكان، كما أنه قادر على الانتقال من جهاز إلى آخر بسرعة كبيرة، ومما زاد من خطورته التقدم الكبير في وسائل الاتصال حيث أدى إلى سهولة الاتصال بين أجهزة الحاسوب (داود، 2000).

أنواع الفيروسات

ويذكر القحطاني (2008) أن للفيروسات أنواعا كثيرة، وفيما يلي أهم الأنواع الرئيسية الأكثر انتشاراً:

1. فيروسات بدء التشغيل (الإقلاع) (Boot Sector Viruses): تصيب عملية بدء التشغيل في القرص الصلب. ويتم توجيه الجهاز لتنفيذ الكود الخاص بالفيروس بدلا من استكمال الحاسوب بالعمل وبالتالي تفشل عملية الإقلاع .
2. فيروسات الملفات (File Infecting Viruses): تستطيع هذه الفيروسات إصابة جميع الملفات بمختلف أنواعها، وغالباً ما ينتج عنها زيادة حجم الملفات.
3. الفيروسات الجزئية الكبيرة (Macro Viruses): تستخدم البرمجة الخاصة بتطبيق معين للبدء بعملها، وتضرب ملفات البيانات (مثل وورد وإكسل)، وتختلف عن فيروسات الملفات في أنها تصيب ملفات البيانات فقط.
4. فيروسات البريد الإلكتروني: تنتقل هذه الفيروسات عبر البريد الإلكتروني، وأصبح انتقالها عبر العالم سهلا جدا وخلال ساعات. ومن أشهرها فيروس ماليسا (Malissa).

وتقسم الفيروسات من حيث تكوينها وأهدافها إلى:

1. فيروس عام العدوى: وهو الفيروس الذي ينتقل إلى أي برنامج أو ملف.

2. فيروس محدود العدوى: وهو الذي يستهدف نوعا معينا من النظم لينتقل إليه ويهاجمه، ويتميز عن النوع السابق بأنه أبطأ بالانتشار وأصعب في الاكتشاف.
3. فيروس عام الهدف: وهذا النوع سهل إعداده ومدى تخريبه أكبر، لذلك فغالبية الفيروسات التي تم اكتشافها تندرج تحت هذا النوع.
4. فيروس محدود الهدف: وهذا النوع من الصعب إعداده لأنه يحتاج إلى كفاءة ودراية كبيرة بالتطبيق والهدف الذي يستهدفه (سلامة، 2006).

وأشار الجواد والفتال (2008) إلى أن الفيروسات تتصف بالصفات التالية:

1. القدرة على الانتشار: وساعد على ذلك تطور وسائل الاتصال التي مكنته من الانتقال بسرعة كبيرة إلى ملايين المستخدمين.
2. القدرة على الاختفاء: بعض الفيروسات تدخل الحاسوب كملفات مخفية (Hidden Files) بحيث لا يستطيع المستخدم ملاحظتها، وبعضها تستقر في الذاكرة وتبقى حتى تاريخ معين لتقوم بتشغيل نفسها وتبدأ بالتدمير، وهناك فيروسات تخفي أي أثر لوجودها حيث تبقى البرامج تعمل بكفاءة لفترة طويلة بالوقت الذي ينتقل فيه الفيروس من برنامج لآخر.
3. القدرة على التدمير: من الممكن أن يحمل الحاسوب برنامجا يرتبط به الفيروس ويبقى ساكناً حتى يجد حافزا يجعله يبدأ بالتدمير.
4. القدرة على الاختراق: بإمكان الفيروس اختراق المواقع التي يقوم المستخدم نفسه بتحميل هذه البرامج منها إلى النظام دون أن يشعر.

وقد تكون الأضرار الناجمة عن وجود الفيروس محدودة عندما يكون تأثيره مقتصرا على إزعاج المستخدم، وتكون إزالته سهلة ويمكن إصلاح آثاره بسهولة أيضا. وقد تكون آثاره متوسطة مثل تسببه في تعطل بعض البرامج التطبيقية مما يلزم إعادة تثبيتها من جديد. ومن الممكن أن تكون آثار الفيروس شديدة مثل الكتابة على القرص الصلب كما يفعل الفيروس (Michelangelo) الذي يكتب معطيات غير مفيدة فوق القسم الأكبر من القرص الصلب (حجار، 2003).

وذكر القحطاني (2008) عددا من الأعراض التي تصاحب وجود الفيروسات منها:

1. البطء الشديد: حيث يعمل الجهاز ببطء ملحوظ وتصبح سرعة البرامج أبطأ من المعتاد، ويلحظ ذلك عند بداية وإيقاف التشغيل، وسببه نقص شديد في الذاكرة العشوائية (RAM).
2. تجمد (تعليق) الحاسوب: يدخل الحاسوب في حالة من الجمود وعدم الاستجابة لأي أمر ولا يمكن تشغيل أي برنامج في الجهاز.
3. انهيار الحاسوب: في أغلب حالات الانهيار تظهر شاشة غريبة ويتوقف الجهاز عن العمل.

4. إضاءة لمبة القرص الصلب بشكل عشوائي ومتصل.
5. وزيادة الزمن اللازم لتشغيل البرامج وفتح الملفات وزيادة حجمها.
6. تلف البيانات التي كانت صالحة من قبل.
7. ظهور رسائل خطأ ومربعات حوار غير متوقعة.
8. إعادة تشغيل الجهاز بشكل آلي ومستمر.

تصنيف البرمجيات الماكرة (MALWAR):

بشكل عام يقسم الجواد والفتال (2008) البرامج الماكرة إلى أربعة أنواع رئيسية، هي: الفيروسات (Viruses)، والديدان (Worms)، وأحصنة طروادة (Trojan Hourses)، وبرامج الانزال (Droppers):

1. الفيروس: مصمم ليقترن ببرنامج آخر ويعمل عندما يعمل ذلك البرنامج ومن ثم يعيد إنتاج نفسه، وقد يغير نفسه ليظهر بنسخة معدلة كلما كرر العملية.
2. الديدان: تختلف عن الفيروسات في أن الفيروس يكرر نفسه بواسطة برنامج مصاب، أما الديدان فتستغل فجوات في نظام التشغيل للقيام بهجومها وهي لا تلوث برامج أخرى، إذ تنسخ نفسها على الأقراص المرنة أو عبر الشبكات.
3. أحصنة طروادة: تختبئ ضمن برامج يبدو مظهرها بريئاً وعند تشغيلها بظهر الجزء الماكر.
4. برامج الإنزال: مصممة لمراوغة برامج مكافحة الفيروسات، وتقوم بنقل وتركيب الفيروسات، فهي تنتظر لحظة حدوث أمر معين حتى تنطلق وتنشر الفيروس المحمول في طياتها، وتنتمي القنابل (Bomb) إلى هذه الفئة التي تبرمج لتنطلق عند حدوث أمر معين في وقت معين.

مكافحة الفيروسات

إن الحماية من الفيروسات تعتبر عملا ضخما وكبرى شركات الحاسوب لها منتجات لبرامج محاربة الفيروسات، وكثير من دول العالم بها قوانين ضد تقديم فيروسات خبيثة، وعلى الرغم من ذلك فهناك العديد من الفيروسات والعديد من الحوادث سنويا. وأشار القحطاني (2008) إلى إمكانية مكافحة البرامج الضارة من خلال حزمة واحدة لمكافحة الفيروسات والديدان وأحصنة طروادة، ولا بد أن تشتمل (ليس فقط)على كشف الإصابات وإنما إزالتها أيضاً، ومن الأمثلة عليها: حزمة برامج سيمانتك (Symantec)، وكاسبر سكاي (Kasper SKY)، ونورتون (NORTON)، ومكافي (Mcafee)، ولا بد من اتباع الخطوات التالية من أجل المكافحة الجيدة:

1. تحديث برنامج المكافحة بشكل آلي ودوري لضمان كشف وإزالة الفيروسات.

2. تحديث نظام التشغيل بشكل دوري عن طريق خاصية التحديث التلقائي لتلاشي الثغرات الأمنية عند وجودها.
3. تحميل ملفات الإصلاح الأمني الخاصة بأنظمة التشغيل وبعض البرامج الأخرى (كالأوفيس)
4. عدم فتح مرفقات البريد الإلكتروني التي لها الامتدادات التشغيلية مثل: (exe,scr,vbs)، أو التي لها أكثر من امتداد مثل: (txt.vbs).

ويمكن أن تعمل برامج المكافحة على إحدى أو جميع الطرق التالية (بانكس، 2001):

1. البحث ضمن البرامج المشبوهة عن وجود فيروسات في الرسائل الواردة أو فيروسات تقوم بعمليات أو وظائف تضر البيانات مثل أمر الحذف (Delete) وإعادة التهيئة (Format).
2. التحقق من وجود تغيرات في ملفات النظام، وحجز البرامج التي يشتبه بوجود فيروس ضمنها وعزلها بحيث لا يمكن تنفيذها قبل التخلص من الفيروسات .
3. إصلاح الملفات المتضررة بسبب الفيروسات وفحص الملفات التي يتم تحميلها والملفات المرفقة للبريد الإلكتروني وفحص المجلدات والملفات ضمن جدول زمني.
4. تحديث البرامج لنفسها عند الطلب أو بشكل آلي، وحماية النظام والبرامج والملفات بشكل آلي.

إجراءات حماية المعلومات

ويرى داود (2000) أن هناك عدة إجراءات وقائية يمكن أن تقوم بها المؤسسات لتجنب كثير من العواقب الوخيمة التي تترتب على الإصابة بالفيروسات، وهي:

1. إعداد النسخة الأصلية من البرامج المشتراة وحفظها بمكان آمن لاسترجاعها وقت الحاجة.
2. الاحتفاظ بسجل لكل عمليات التعديل في برامج االتطبيقات حيث يتم تسجيل جميع وقائع نقل البرامج المعدلة.
3. توعية العاملين بالمؤسسة بعدم تحميل أي برنامج من الخارج، فهذا أوسع الأبواب لإدخال الفيروسات إلى النظم والتي عند دخولها قد تصيب جميع الأجهزة بالشبكة.
4. عدم السماح بالاستخدام العام للبرامج في المؤسسة، إلا بعد التأكد من خلوها من الفيروسات.
5. تركيب برنامج على الشبكة الداخلية للتحقق من وجود فيروسات ويفضل أن يكون دائما.
6. اتخاذ إجراءات في مواجهة المتصلين من خارج المؤسسة للتأكد من خلو البرامج المدخلة من جانبهم من الفيروسات.
7. تدريب الموظفين على كيفية الوقاية من الفيروسات والتعامل معها عند العثور عليها .
8. أخذ نسخ احتياطية من البيانات على فترات منتظمة وحفظها في مكان آخر.
9. تحديد مسؤولية التعامل مع البيانات وتسجيل وقائع استخدام الملفات وقواعد البيانات .

10. نشر اجراءات محددة وواضحة على المستفيدين لاتباعها في حالة ظهو فيروس لديهم.

11. عدم السماح بنقل الملفات أو البرامج على أقراص لاستكمال أعمالهم في المنزل.

أمن الشبكات

العديد من المؤسسات وأكثرها تطورا عانت من مشاكل في حماية شبكاتها فليس هناك ضمان ولا ثوابت تمنع احتمالية اختراق الأجهزة، ولكن هناك عوامل تقلل من هذه الاحتمالية، وهناك مراقبة بمجرد الدخول للشبكة العنكبوتية بقصد أو بدون قصد وليست كلها ضارة بمجرد الدخول للشبكة، وأبرز الذين يقومون بالمراقبة هم مزودو خدمة الاتصال بالإنترنت، فهم من يمتلكون السيطرة عليك وعلى بياناتك لأن اتصالك يمر من خلاله، وإن معظم البيانات التي يتم جمعها تستخدم لأسباب أمنية ولا يطلع عليها إلا للضرورة (رمضان ، 2009).

الشبكات هي ربط جهازين أو أكثر وذلك لتبادل المعلومات، ويمكن أن يكون من خلال حاسب شخصي أو مركزي بالإضافة إلى المنافذ والطرفيات والأجهزة الأخرى مثل الطابعات وغيرها. بالإضافة إلى البرمجيات المسؤولة عن إدارة العمليات والأجهزة داخل الشبكة. وبناء على هذا الأساس يمكن تحويل البيانات والمعلومات والرسائل بين هذه الأجهزة المتصلة بالشبكة أو شبكات أخرى متصلة بتلك الشبكة. وبناء على ذلك فإن أي شبكة تحتاج للقيام بعملياتها إلى وحدة إرسال، وهذه مسؤولة عن إرسال البيانات والمعلومات إلى الأجهزة الأخرى، ووحدة استقبال تستقبل البيانات والمعلومات والرسائل من الأجهزة الأخرى، ووحدة اتصال لنقل وتبادل البيانات والمعلومات بين الأجهزة المتصلة بالشبكة (خطاب، 2006).

هناك عدة طرق ووسائل لحماية الأنظمة من التعرض للهجمات ومنع استغلال نقاط الضعف فيها، كتركيب برامج خاصة لجعل استخدام الإنترنت أكثر أمانا لك، وسنستعرض فيما يلي الوسائل والبرمجيات التي تسهم في إبقاء المعلومات آمنة قدر الإمكان (رمضان، 2009):

- وسائل الحماية المادية: عن طريق وضع الحواسيب في أماكن آمنة، وتحمى بكلمات مرور وعدم إفشاء هذه الكلمات .
- التحديثات الدورية: تحديث جميع البرامج بما في ذلك أحدث النسخ من نظم التشغيل، أو استخدام التحديث التلقائي.
- جدران النار (Firewall): تنقسم جدران الحماية النارية إما لبرامج أو أجهزة خاصة تستخدم لحماية الشبكة والسيرفر من المتسللين، وتختلف جدران النار حسب احتياجات المستخدم، فإذا استدعت الحاجة إلى وضع جدار النار على عقدة منفردة عاملة على شبكة واحدة فإن جدار النار الشخصي هو الخيار المناسب، وفي حالة وجود حركة مرور داخلة

وخارجة من عدد من الشبكات، فيتم استخدام مصاف لجدار النار في الشبكة لتصفية الحركة المرورية.

- برامج مراقبة بيانات الشبكة (Packet Sniffers): يتم من خلالها تجميع البيانات الداخلة والخارجة، تعتبر من أكثر برامج مراقبة بيانات الشبكة حساسية ودقة، وهي طريقة ممكن أن تكون مفيدة في الكشف عن محاولات التسلل عبر الشبكة، وكذلك يمكن استخدامها لتحليل مشاكل الشبكة وتصفية وحجب المحتوى المشكوك فيه من دخول الشبكة.
- التشفير: ترميز البيانات كي تتعذر قرائتها من أي شخص ليس لديه كلمة سر لفك شيفرة تلك البيانات، ويجعل التشفير المعلومات في الجهاز غير قابلة للقراءة من قبل أي شخص يستطيع أن يتسلل خلسة إلى جهازك دون إذن. ويقوم التشفير بمعالجة البيانات باستخدام عمليات رياضية صعبة.
- بروتوكول (Kerberos): عبارة عن بروتوكول لإثبات شخصية شبكات الحاسوب، وقد صمم لتوفير إثبات شخصية قوي لتطبيقات الخادم والمستفيد باستخدام تشفير المفتاح العام. وهو متوفر في معهد ماشيتسر للتكنولوجيا وفي بعض التطبيقات التجارية. ويحتوي على قاعدة بيانات يخزن فيها (بيانات المستخدمين، والخدمات المتوفرة، والسيرفرات، والمفاتيح العمومية).
- ويضيف المصري (2008) ضرورة التأكد من عدم وجود التروجان وهو خادم يسمح للمخترق عبر الشبكة بالتحكم في الأجهزة، ويتم ذلك من زرعه بالجهاز عن طريق رسائل البريد الإلكتروني مثلا أو عن طريق قرص مرن أو من خلال العبث في برامج الاختراق.

تهديدات الشبكات (Threats in Networks)

إن الشبكات لا تخلو من التهديدات الأمنية التي تواجهها نتيجة لمبدأ تصميمها الذي لم يأخذ بعين الاعتبار النواحي الأمنية، فهي مصممة بالأساس لتبادل الأبحاث العلمية، ولم يكن متوقعا أن يتم استخدام هذه الشبكات في التجارة والتعليم والأعمال التجارية، وفيما يلي ملخص لأهم المشاكل الأمنية التي تواجه الشبكات (الطيطي،2010):

1. المشاركة (Sharing): إن العديد من المستخدمين لهم القدرة على الوصول إلى الأنظمة الموجودة على الشبكة، لأن مصادر الشبكة من أجهزة وملفات ومجلدات تكون مشتركة وقابلة للاستخدام من العديد من المستخدمين بينما نلاحظ أن المستخدم للحاسبات المنفردة لا يستطيع الوصول إلى المصادر الأخرى لعدم وجود ربط بينه وبين الحواسيب الأخرى.

2. تعقيد النظام (Complexity of System): يستطيع المتطفلون أن ينفذوا إلى النظام للقيام بالأعمال التخريبية عن طريق أخطاء صغيرة غير منظورة وهي ناتجة عن البرمجيات المعقدة.
3. حدود غير معروفة (Un Known Perimeter): عدم التأكد والوثوق من حدود الشبكة من خلال التوسع في الارتباط بالشبكة، فقد يكون أحد المضيفين هو عقدة على شبكتين مختلفتين، لذلك فإن المصادر على الشبكة يمكن الوصول إليها من قبل مستخدمي الشبكات الأخرى، وبالرغم من أن التوسع في الشبكة والوصول إلى البيانات يعتبر واحدا من الفوائد، لكن هذه المجموعة غير المعروفة أو غير المسيطر عليها قد تكون مجموعة مستخدمين ضارة، لذلك تكون هذه الصفة من الناحية الأمنية غير مفيدة.
4. العديد من نقاط الهجوم (Many Point of Attack): إن الملف قد يمر خلال العديد من المضيفين قبل أن يصل إلى المستخدم عندما يتم تخزين ملف في مضيف شبكة بعيد عن المستخدم، لذلك يمكن أن يتم التأثير أو التطفل أو القيام بعملية التغيير على هذا الملف في أي موقع قبل أن يصل إلى الجهة المطلوبة، إضافة إلى أن إدارة الشبكة لا تسيطر على المضيفين الآخرين في الشبكة.
5. المجهولية (Anonymity): يستطيع المهاجم أن ينفذ هجومه من أماكن مختلفة وعلى بعد مئات الأميال، ولذلك فإن هذا المهاجم لا يكون على صلة بأي من الإدارة أو مستخدمي الشبكة فعملية الهجوم يمكن أن تمر من خلال الكثير من المستخدمين الآخرين وذلك لإخفاء الجهة الأصلية المنفذة للهجوم، وأخيرا فإن عملية إثبات الشخصية بالنسبة لحاسوب إلى حاسوب مختلفة عن إثبات الشخصية بين الإنسان والحاسوب.
6. التنصت (Wiretapping): وهي عملية قطع الاتصال سواء كانت سلكية أو لا سلكية والقيام بعملية كشف للبيانات، ومن الممكن أن يتم نشرها من خلال نقلها بين الأطراف المتصلة.
7. انتحال الشخصية (Impersonation): وهو تزييف كلمة المرور من خلال قيام المستخدم أو برنامج بانتحال شخصية مستخدم أو برنامج آخر.
8. القرصنة (Hacking): وهي البحث في الشبكة أو الأنظمة عن نقاط ضعف محددة لاختراقها.
9. منع الخدمة Denial of Service : ويتم ذلك من خلال إغراق الشبكة المحلية بآلاف الرسائل أو مقاطعة الخدمات في الشبكة.

أمن أنظمة التشغيل والبرمجيات

إن حماية أنظمة التشغيل تحتاج لإدارة منظومة الحاسوب والعمل على تقليل أو منع محاولات التلاعب بالثوابت أو المفاتيح المنطقية التي تسيطر على تنفيذ البرمجيات من جهة وعلى إدامة مراقبة نظام التشغيل على مجمل الفعاليات داخل المنظومة من جهة أخرى (الجواد والفتال، 2008).

الحماية التي توفرها أنظمة التشغيل

تمتلك نظم التشغيل برامج داخلية تسيطر على بعض العمليات التي يمكن استغلالها من قبل من يريدون إحداث خلل ما في عمل الحاسب أو تسهيل مهمة أشخاص آخرين للاستفادة غير المشروعة من برنامج معين، وتقوم هذه البرامج أيضا بمنع المستفيد في حالة تجاوزه للصلاحيات المحددة له، وكما هو الحال بالنسبة لتعدد أنواع الحاسبات ونظم تشغيلها فإن عناصر الأمن لنظم التشغيل هي أيضا متباينة، وفيما يلي أهم الإمكانيات المتوفرة في نظم التشغيل ذات الطبيعة الأمنية: (الجواد والفتال، 2008):

- كلمات المرور: يتم استعمال هذا الأسلوب لتمكين المستفيد من الدخول أو التخاطب مع منظومة الحاسب الآلي وتمكنه أيضا من استعمال بعض الملفات وقواعد المعلومات وتتكون كلمات السر من مجموعة من الحروف والأرقام أو كليهما وحسب طبيعة نظام التشغيل لكل حاسبة، ونظرا لأهمية هذه الكلمات على صعيد أمن الحاسبات وأمن الأنظمة العاملة عليها فإن على مستعمل هذه الكلمات أن يعمل باستمرار على استبدالها بين فترة وأخرى أو عند الشك باحتمال سرقتها.
- جدول الصلاحيات: ويدعى أيضا بجدول الأمنية، وهو عبارة عن جدول يقوم نظام التشغيل مع برامج أخرى ملحقة به للسيطرة على تنفيذه، ويتباين شكل وتركيب عمل جدول الصلاحيات من حاسبة إلى أخرى، إلا أنها تجمع على سؤال أو أسئلة توجهها الحاسبة بعد إدخال كلمة المرور الصحيحة عن الرمز الممنوح للمستفيد الذي يقوم استخدام برنامج معين. وعند عدم تمكنه من إعطاء هذه المعلومات يقطع الاتصال به مع التنبيه المشغل عن طريق رسالة على شاشة (console) وفي الحالة الاعتيادية يزود كل مستفيد برمز خاص به يحدد خلاله بالفعاليات التي يسمح له بها نظام التشغيل.

ويؤكد الجواد والفتال (2008) أن الحاسوب لا يمكن اعتباره نظاما محميا ان لم يكن هناك تكامل أمني يشمل الأجهزة والبرمجيات على حد سواء، ويجب ان يكون هناك تعليمات مركزية بشأن كتابة البرامج، خصوصا التي تخص أمن المعلومات وعدم كتابة أي برنامج من

شأنه التجاوز على الخواص الأمنية للحاسوب. ولكي تكون البداية صحيحة في تصميم أي نظام لا بد من تحديد طبيعة وشخصية المستفيد، وذلك يتطلب ما يلي:

- تحديد نوع المعلومات المتداولة ودرجة تصنيفها.
- تحديد الجهات أو الأشخاص الذين يتعاملون مع هذه المعلومات وتحديد درجة الثقة بهم.
- إعداد برامج لها القابلية للتمييز بين من يحق له الاطلاع الشامل أو الاطلاع الجزئي أو صلاحية التعديل أو الإدخال فقط بالاعتماد على كلمات المرور.

التوثيق الأمني

إن أمن الأنظمة والبرمجيات لا يقتصر على طبيعة النظام والبرامج المكتوبة له بل يجب أن يشمل أيضا التوثيق المستخدم في إعداد الأنظمة قي جميع مراحله وما يتخلف من عملية طبع المعلومات وعملية خزن هذه المطبوعات بسرية كاملة، وتشمل الحماية أيضا الأشرطة والأقراص المغناطيسية من سوء التداول والفقدان والسرقة، وقد تستدعي بعض الحالات وجود أحد الأشخاص المخولين من قبل الجهة المستفيدة بالقرب من المشغل في حالة تحمل أو رفع أحد الأشرطة أو الأقراص بالغة الأهمية.

التشفير

يعرفه رمضان (2009) بأنه "عملية الحفاظ على سرية المعلومات (الثابتة منها والمتحركة) باستخدام برامج قادرة على تحويل وترجمة تلك المعلومات إلى رموز بحيث إذا ما تم الوصول إليها من قبل أشخاص غير مخول لهم بذلك لا يستطيعون فهم أي شيء لأن ما يظهر لهم هو خليط من الرموز والأرقام والحروف غير المفهومة".

إن الشبكات كثيرا ما تتعرض لاستخدام غير قانوني من خلال مستخدمين أعداء، وهذه الشبكات بمكوناتها لها تهديدات أمنية تجعل من الصعب حماية المعلومات المرسلة بالطرق التشغيلية المعروفة، ولذلك يتم استخدام طريقة التشفير التي تمكن من إبعاد النشاط غير القانوني. وتهدف هذه الطريقة إلى حماية شبكة الاتصال من التأثير لمثل هذه النشاطات (أحمد وخلف، 2002).

جميع الأفراد أو الهيئات لديهم خصوصيات وأسرار ومعلومات هامة جدا لا يجب أن يطلع عليها أحد، كما انه لا يمكن الاستغناء اليوم عن خدمات الإنترنت مثل البريد الالكتروني والتسويق التجاري عبر مواقع التجارة الإلكترونية. وعلم التشفير اكتسب أهمية بالغة منذ مطلع القرن العشرين؛ إذ تبين أن الحربين العالميتين الأولى والثانية كانتا حرب تشفير في المقام الأول. ومنذ

منتصف عقد السبعينيات من القرن العشرين امتد استعمال التشفير ليتعدى الاتصالات والمراسلات العسكرية والدبلوماسية ويصل إلى عدة مجالات واستخدامات أخرى كما يلي: (رمضان، 2009)

- في الصناعة والتجارة: للمحافظة على الأسرار التجارية والعلمية والوضع المالي.
- في البث التلفازي: حيث يتم تشفير المحطات التلفازية حتى لا يستطيع مشاهدتها إلا المشتركون الذين يدفعون اشتراكا شهريا.
- في المصارف: وذلك للحفاظ على حسابات المودعين وحمايتها من التلاعب أو الاختلاس مع تطور الخدمات المصرفية الإلكترونية.
- في شبكات الحواسيب: للمحافظة على المعلومات الحساسة وحماية الملفات والمعلومات وحماية الدخول إلى الشبكات عن طريق الرقم السري الخاص بالمستخدم المصرح له.
- في حماية الاتصالات السلكية واللاسلكية من الالتقاط أو التصنت والاطلاع على أسرار الآخرين الشخصية والعائلية.

ويرى رمضان (2009) أن هناك متطلبات ومعايير يتطلبها أي نظام تشفير كما يلي:

1. يؤدي الوظيفة المطلوبة (Functionality): وهي دمج الأوليات البنائية الأساسية وذلك لتأمين أهداف أمن المعلومات المتعددة في هرم أمن المعلومات، ويتم اختيارها من خلال فعاليتها عن غيرها من الأوليات.
2. الكفاءة في العمل (Efficincy): يشير هذا المعيار إلى مقدرة أو كفاءة وحدة البناء الأساسية في نمط محدد من العمل. على سبيل المثال يمكن أن تقيم سرعة عمل خوارزمية تشفير ما بعدد البتات التي تشفرها خلال ثانية واحدة.
3. مدى ودرجة الأمان المطلوب (Level of Security): غالبا ما يعطى بدلالة عدد العمليات المطلوبة، لذلك فهذا المعيار من الصعب تحديده أو قياسه.
4. سهولة التطبيق (Easy of Implementing): يشير هذا المعيار إلى صعوبة تحقيق وحدة البناء الأساسية المقصودة في وضع تعيين علمي، وهذه عادة ما تتضمن مقدار تعقيد التنفيذ لوحدة البناء هذه سواء في بيئة مكونات برمجية أو مادية.
5. طرق العمل (Methods of Operation): عندما تطبق هذه الوحدات البنائية الأساسية فإنها ستقدم مهمات وظيفية مختلفة اعتمادا على نمط عمله أو استخدامه.

ويرى الطيطي (2010) أنه لكي تكون عملية التشفير آمنة وفعالة لا ابد من توفر أمرين أساسيين هما:

1. خوارزمية تشفير قوية: بحيث تفقد الخصم القدرة على فتح النص المشفر أو كشف المفتاح وإن كان مطلعا لعدد من النصوص المشفرة سوية مع النص الواضح الذي ينتج النص المشفر.
2. يجب أن يحصل المرسل والمستلم على نسخ من المفتاح السري وبطريقة أمينة ويجب أن يحافظا على سرية المفتاح بقدر عالٍ من الحرص، حيث إنه إذا تمكن شخص من اكتشاف المفتاح ومعرفة الخوارزمية، فستصبح جميع الاتصالات التي تستخدم هذا المفتاح مكشوفة.

وهناك أنواع عديدة من برامج التشفير؛ منها المجانية ومنها التجارية ومنها الشخصي ومنها على مستوى المنظمات والمؤسسات، وهناك اختلاف في طريقة عمل كل واحد منها فبعضها يشفر ملفا وبعضها يتيح تشفير مجلد كامل بما فيه، وبعضها يتيح أوعية تمكن من وضع الملفات المراد تشفيرها فيها وهي تقوم بالتشفير التلقائي، ومن الأمثلة على برامج التشفير (Best Crypt) الذي يقوم باحتجاز مساحة محددة من القرص الصلب ويكون ما يعرف بالوعاء المشفر، وبرنامج (Fine Crypt) الذي يحتوي على العديد من المميزات مما يثري عمل البرنامج وفي الوقت نفسه يعقد عمله.

وهناك عناصر مهمة للشفرة الجيدة أشار لها الطيطي (2010):

1. يجب أن تحدد حجم السرية المطلوبة وحجم العمل المناسب للتشفير، والمبدأ الأول هو إعادة تكرار مبدأ استغلال الوقت.
2. يجب أن تكون مجموعة المفاتيح وخوارزمية التشفير خالية من التعقيد، وهذا يعني بأننا يجب ألا نحدد اختيارا للمفاتيح أو نوع النص الواضح الذي ستطبق عليها الخوارزمية.
3. يجب أن يكون تنفيذ العملية بسيطا قدر الإمكان: تم وضع المبدأ الثالث آخذين بعين الاعتبار أن يكون التنفيذ يدويا وبدون استخدام الآلة، حيث إن استخدام خوارزمية معقدة يؤدي إلى وجود أخطاء، ومع تطور وكثرة استخدام الحواسيب الرقمية أصبحت الخوارزميات أكثر تعقيدا ومن غير الممكن تنفيذها يدويا ولا يزال موضوع التعقيد من المواضيع المهمة، حيث إن كثير من المستخدمين يتجنبون خوارزميات التشفير المعقدة حتى وإن كانت ذات كفاءة كبيرة من الناحية الأمنية.
4. يجب ألا ينتشر الخطأ في التشفير ليسبب تدميرا أكثر لمعلومات الرسالة: يوضح المبدأ الرابع بأن الإنسان سوف يقع في خطأ عند استعماله لخوارزميات التشفي، حيث إن الخطأ الذي يحصل في بداية العملية يجب ألا يؤدي إلى إلغاء النص الواضح الباقي بكامله، فمثلا حذف

حرف واحد في طريقة العمود الإبدالي سوف يؤدي إلى إلغاء التشفير الباقي بأكمله إلا إذا استطاع المستلم أن يخمن أين يقع الحرف المحذوف، فسوف يعرف بقية الرسالة.

5. يجب ألا يكون حجم النص المشفر أطول من النص الأصلي للرسالة. إن الفكرة وراء المبدأ الخامس هي أن النص المشفر إذا كان حجمه كبيرا جدا فإنه من المحتمل ألا يحمل معلومات أكثر من النص الواضح، وكذلك فإنه يعطي الفرصة لمحلل الشفرة أن يطلع على بيانات أكثر يمكن منها أن يستنتج نموذج التشفير. أكثر من ذلك، فإن النص المشفر الأطول يؤدي إلى زيادة حجم البيانات المحفوظة وكذلك وقت أطول للاتصال.

النسخ الاحتياطي

إنه من الضروري وجود طريقة تمكننا من استعادة البيانات التالفة أو المفقودة لضمان مستوى أعلى من الحماية، وبالرغم من الإجراءات الاحتياطية إلا أنه يوجد احتمالية لحدوث تلف أو تحريف أو فقدان للمعلومات. فالنسخ الاحتياطي يحقق هذا المستوى من الحماية من خلال إنشاء نسخ يتم حفظها سواء داخل المقر أو خارجه، ولضمان أقل قدر من الخسائر عند فقدان البيانات الأصلية يتم تحديثها باستمرار. ويجب تحديد ما ينبغي نسخه، حيث عادة ما يشمل كل المعلومات التي يصعب إعادتها مثل المعلومات الأساسية والحيوية الخاصة بالنظام وقواعد البيانات وغيرها. ويتم النسخ الاحتياطي على فترات يومية أو أسبوعية أو شهرية وفقا لما يلائم العمل ولا بد ان يكون النسخ دوريا على فترات منتظمة يتم تحديدها مسبقا لا عشوائيا حتى معرفة الفترة التي يجب الرجوع اليها في حال حدث أي خلل(بامفلح، 2003).

يوجد أنواع مختلفة من النسخ الاحتياطي مثل النسخ الاحتياطي الكامل الذي ينسخ جميع الملفات للنظام والبرامج والبيانات، ويفترض أن تتم عملية النسخ أسبوعيا أو شهريا، وفي حال حدوث أي خلل للملفات الأصلية يمكن استعادة كامل النظام. وهناك نسخ احتياطي جزئي يمكن من نسخ جميع الملفات التي تمت إضافتها أو تغيرت منذ آخر عملية نسخ (الكردي، 2011).

وحددت أكاديمية الفيصل التعليمية (2008) عدة طرق لعمل النسخ الاحتياطي:

1. إجراء النسخ الاحتياطي الروتيني للحاسوب بأكمله أو لمجلدات أو ملفات فردية.
2. إجراء نسخ احتياطي أوتوماتيكي من خلال برامج خاصة وفي أوقات معينة.
3. حفظ النسخ الاحتياطية في مكان آمن بعيد عن الأخطار والحريق وضوء الشمس والمجالات المغناطيسية.
4. عمل نسخ عديدة وتوزيعها في أماكن مختلفة.

5. وضع ملصق على الأقراص يسجل فيها معلومات عن محتواها.
6. الاحتفاظ بالأقراص في وضعية محمي من الكتابة Write-Protected.

حقوق النشر والتوزيع

تعرفها أكاديمية الفيصل العالمية (2008) على أنها لحق القانوني الذي يمكنك من إعادة إنتاج ونشر وبيع المحتوى وكل أشكاله. وتنطبق حماية هذه الحقوق على البرامج الكاملة والملفات الفردية أو بعض أجزاء الملفات مثل النص أو الرسم أو الفيديو أو الصوت. ولا يعني شراء البرمجية الحصول على حق الملكية وإنما الحصول على رخصة استخدام، وهذه الرخصة لها شروط تسمى (Lincensing Agreement) وتكون مكتوبة في توثيق البرمجية أو الغلاف الخارجي للأقراص أو تظهر عند فتح البرمجية على الشاشة، ولا بد من الموافقة عليها. ولهذه الرخصة نوعان:

- رخصة المستخدم الواحد (Single User License): ويعني استعمالها من قبل شخص واحد على حاسوب واحد.
- رخصة متعدد الاستخدام (Sit Licese): تسمح هذه الرخصة تحميل البرمجية على عدة حواسيب محدد عددها بالرخصة، ويحصل ذلك مثلا عند وجود أكثر من مستخدم ضمن المؤسسة يرغبون باستخدام برنامج واحد.

المكتبة الجامعية

مفهوم المكتبة الجامعية

تعرف المكتبات الجامعية بأنها المكتبات التي تنشؤها الجامعات وتقوم بتمويلها وادارتها وذلك لخدمة المجتمع الأكاديمي المكون من الطلبة والمدرسين والإداريين العاملين في الجامعة وكذلك المجتمع المحلي من خلال تقديم المعلومات والخدمات المكتبية المختلفة للمجتمع. كما يمكن أن يكون هناك مكتبة مركزية واحدة، ومن الممكن أن يكون بالإضافة إلى المكتبة المركزية عدد من المكتبات الفرعية أو مكتبات الكليات المرتبطة إداريا وماليا بالمكتبة المركزية للجامعة (عليان، 2014).

ويعرفها إبراهيم (2009) بأنها مؤسسة ثقافية وعلمية وتربوية تعمل على خدمة المجتمع الجامعي من طلبة وأساتذة وباحثين من خلال توفير ما يحتاجونه من مصادر المعلومات بعد

تنظيمها وتصنيفها وفهرستها وتكشيفها ليسهل الوصول إليها، وهي جزء أساسي من المؤسسة التعليمية التابعة لها.

أهمية المكتبة الجامعية

إن المكتبات الجامعية من أهم ركائز التعليم الجامعي وتحظى باهتمام كبير ودعم مادي ومعنوي من قبل المسؤولين وأصحاب القرار في معظم الجامعات، لما تقدمه من نشاطات في تشجيع البحث العلمي ودعم المنهاج الدراسي والبرامج الأكاديمية الأخرى، وتعتبر من أهم مرافق الجامعات إن لم تكن أهمها على الإطلاق من خلال توفير مصادر المعلومات بأشكالها وأنواعها المختلفة، سواء كانت هذه المصادر تقليدية أو إلكترونية أو سمعية وبصرية، ولذلك فإن مسؤولية تنمية وتطوير هذه المكتبات هي مسؤولية مشتركة تقع على عاتق رئاسة الجامعة وإدارة المكتبة والعاملين فيها وعلى المستفيدين منها، لكي تكون في النهاية مكتبات جامعية متطورة تحقق أهداف المكتبة من ناحية وتحقيق رسالة الجامعة العلمية من ناحية أخرى(عليوي والمالكي 2007).

فمن خلال ما توفره المكتبة من خدمات ومصادر معلومات فإنها تلعب دورا كبيرا في خدمة البحث العلمي وتطويره، حيث تضم هذه المكتبات عددا من المصادر الحديثة في كافة التخصصات التي لا يستطيع الباحث اقتناءها أحيانا لارتفاع ثمنها، وتقدم المكتبات الجامعية خدمات مهمة لإفادة الباحث أو المستفيد والتسهيل عليه في البحث واسترجاع المعلومات مثل الخدمات المرجعية والتكشيف والإحاطة الجارية والبث الانتقائي والبحث بالاتصال المباشر بالإضافة لخدمات الفهرسة والتصنيف والتزويد وغيرها وغيرها من الخدمات التقليدية والمحوسبة.

وفي ظل التغيرات التكنولوجية لم تعد المكتبة الجامعية بشكلها التقليدي قادرة على الوفاء باحتياجات المستفيدين، وظهرت الحاجة إلى جعل المكتبات الجامعية مراكز وأجهزة للمعلومات تقوم بعمليات الاختيار والانتقاء والتحليل والتنظيم والخزن والاسترجاع لتلك المعلومات وحسب احتياجات المستفيدين نتيجة للتطور الحاصل وتزايد مصادر المعلومات وتنوع الخدمات التي ينبغي توفيرها، من خلال إضافة بعض الخدمات إلى خدماتها التقليدية المنشورة وكذلك مشاركة المكتبة بشبكات المعلومات المحلية والإقليمية عن طريق مشاركة المصادر وتقديم خدمات شبكة الانترنت وتوفير المستلزمات المادية والبشرية لها والتي من شأنها أن تفعل دور المكتبة في الحصول على المعلومات والمساهمة في عمليات التحرير والنشر والترجمة والتصوير واستخدام الحاسبات الإلكترونية في معالجة وإنتاج هذه الخدمات وتقديمها لرواد المكتبة بأيسر الطرق وأسرعها، وهذا يجعل المكتبة الجامعية قادرة أن تؤدي دورها بشكل كامل لكي تسهم في العملية

التربوية والعلمية والثقافية والحضارية ولتكون مركز استقطاب للطلبة والأساتذة للإفادة من خدماتها ونشاطاتها المختلفة (عليوي والمالكي 2007).

وظائف المكتبة الجامعية

إن وظائف المكتبات الجامعية تنبع من وظائف وأهداف الجامعات، ولعل الوظيفة الرئيسية للمكتبات الجامعية هي توفير مصادر المعلومات بمختلف أنواعها وأشكالها وإعدادها فنيا لتسهيل الوصول إليها بأقل وقت وجهد وتسهيل استخدامها وطرق استرجاعها (إبراهيم، 2012). وأشار همشري (2009) إلى عدة وظائف للمكتبة الجامعية:

1. توفير مصادر المعلومات ذات العلاقة الوثيقة بالتخصصات المتوافرة والبرامج الأكاديمية والبحوث الجارية في الجامعة.
2. تنظيم مصادر المعلومات من خلال القيام بالعمليات الفنية اللازمة وذلك لتسهيل الوصول لها.
3. خدمة مجتمع المستفيدين من خلال الإعارة والمراجع والدوريات والتصوير والإرشاد وغيرها.
4. تدريب المستفيدين على استخدام المكتبة ومصادرها وخدماتها المختلفة.
5. تجميع البحوث والدراسات العلمية التي يقوم بها أعضاء هيئة التدريس والطلبة وتوزيعها والإعلام عنها وإهداؤها والتبادل بها.
6. تدريب العاملين في مجال المكتبات والمعلومات من المجتمع المحلي.
7. تطوير العلاقة مع المكتبات الأخرى وخصوصاً الجامعية من خلال شبكات المكتبات وغيرها.

مقومات المكتبة الجامعية

وأشارت موسى (2012) إلى عدد من المقومات المادية والبشرية التي تحتاجها المكتبة الجامعية لتحقيق أهدافها التعليمية والبحثية بفاعلية، تتمثل في:

1. المقومات المادية وتشمل موقع المكتبة حيث يؤثر تأثيرا أساسيا في التردد على المكتبة، فالموقع الجيد أحد أهم المقومات في تقديم الخدمات المكتبية بشكل فعال، وكذلك المبنى فلا يمكن أن تؤدي المكتبة الجامعية دورها بدون مكان مناسب يستوعب مجموعاتها وتجري فيه العمليات والإجراءات والخدمات المكتبية، ويعد الأثاث والتجهيزات من المقومات الهامة، وتضم الرفوف ومكاتب الموظفين والمقاعد والملفات وغبرها، ومن المقومات المادية أيضا وجود مجموعات مميزة من الكتب والدوريات والمخطوطات والمراجع وغيرها.
2. المقومات البشرية، فالمكتبات الجامعية تحتاج عددا كافيا من المؤهلين للعمل مع المجتمع الجامعي لمساعدته في إشباع حاجاته من المعلومات، وإدارة ناجحة ونشيطة وفعالة وقادرة على الاتصال مع الأطراف الإدارية والأكاديمية في الجامعة، ودعما ومساندة معنوية ومادية من إدارة الجامعة .

مقتنيات المكتبة الجامعية

إن مقتنيات المكتبة الجامعية واسعة ومتعددة شكلا وموضوعا؛ وذلك بسبب تنوع برامج الجامعة وخصائص مجتمعها. وعادة تضم مكتبة الجامعة الكتب بأشكالها المختلفة، والدوريات العامة والمتخصصة، والمراجع العامة والمتخصصة، والدراسات والبحوث والرسائل الجامعية، والمواد السمعية والبصرية، والمصغرات الفلمية، المخطوطات والوثائق، والمصادر كافة التي تساعد الطلبة في الدراسة والتحضير وكتابة البحوث والباحثين في إعداد بحوثهم ودراساتهم وأعضاء الهيئة التدريسية في القيام بأعمالهم الأكاديمية المختلفة (عليان، 2014).

مصادر المعلومات في المكتبات الجامعية

يمكن تقسيم مصادر المعلومات في المكتبات الجامعية إلى ثلاثة أقسام: مصادر المعلومات التقليدية، ومصادر المعلومات غير التقليدية ومصادر المعلومات الإلكترونية (ملحم، 2011):

1. مصادر المعلومات التقليدية: وهي مصادر المعلومات ذات الشكل المطبوع، وتتمثل في الكتب التي تعد أكثر هذه المصادر شيوعا واستخداما لسهولة حملها ورخص ثمنها وسهولة تداولها وتصفحها. والدوريات؛ وتضم الصحف اليومية والمجلات العامة والمتخصصة، والمخطوطات وهي من المصادر الأولية الهامة لاحتوائها على معلومات في مختلف صنوف المعرفة ولكونها غير منشورة.
2. مصادر المعلومات غير التقليدية: وتضم المواد السمعية والبصرية والمصغرات الفيلمية وتستخدم هذه المصادر لتوفير الحيز المكاني وتأمين المعلومات ضد السرقة والحفاظ على السرية والتخلص من الصعوبات التي تتعلق بالمطبوعات الورقية
3. مصادر المعلومات الإلكترونية: وهي إحدى ثمرات تكنولوجيا المعلومات وتقنيات الاتصالات التي مكنت من إنتاج وبث المعلومات وإتاحتها للمستفيدين متجاوزة الحدود المكانية والزمانية.

مصادر المعلومات الإلكترونية

يعرفها الشوابكة (2010) بأنها كل أنواع أوعية المعلومات التي تنشأ وتعالج وتبث بواسطة الحاسوب.

عوامل ظهور مصادر المعلومات الإلكترونية

يرى النوايسة (2011) أن هناك عدة عوامل أدت إلى ظهور مصادر المعلومات الإلكترونية، ومنها:

1. العوامل المعلوماتية المرتبطة بسمات الانتاج الفكري، مثل تضخم الإنتاج الفكري وتعدد لغاته وتنوع مصادره وأنواعه وأشكاله وتعقد موضوعاته وتداخلها مع بعضها؛ فهذه العوامل جعلت المكتبات عاجزة عن ملاحقة وحصر هذه المواد المنشورة ومتابعتها يدوياً.

2. العوامل الاسترجاعية: تشمل العوامل المتعلقة باحتياجات المستفيدين، مثل سرعة الحصول على المعلومات، وتوفير الوقت والجهد، وتنوع مصادر المعلومات، والإتاحة الدائمة للمعلومات.
3. العوامل الاقتصادية: وتتمثل في ارتفاع تكاليف مصادر المعلومات التقليدية المطبوعة، وتشمل تكاليف إنتاج وطباعة وتحرير ونشر مصادر المعلومات التقليدية، وارتفاع أسعار الورق والحبر والشحن ونقل المطبوعات، وتكاليف التجليد والصيانة، والبناء والأيدي العاملة، والتجهيزات.
4. العوامل التقنية والتكنولوجية: وتشمل تقنيات المعلومات والاتصالات، وتتمثل في تقنيات الحاسوب، والاتصالات وتراسل البيانات، ونظم الاتصال المباشر، والأقراص المتراصة، والنشر الإلكتروني، وشبكة الإنترنت، والمكتبات الرقمية.
5. العوامل الجغرافية متمثلة في اختفاء مفهوم الحواجز المكانية وإمكانية الحصول على أي معلومة من أي مكان وفي أي وقت.

مميزات مصادر المعلومات الإلكترونية

لقد أشار الخثعمي (2009) إلى مجموعة من المميزات لمصادر المعلومات الإلكترونية جعلتها تحتل مكانة مميزة بين أنواع مصادر المعلومات وزيادة الإقبال عليها سواء من مؤسسات المعلومات أو المستفيدين أنفسهم، ومن أهم هذه الميزات:

1. حداثة المعلومات إذا ما قورنت بمصادر المعلومات التقليدية.
2. السرعة في الحصول على المعلومات وفي أي وقت يتناسب مع المستفيد.
3. تعدد الخيارات للمستفيد في كيفية الاستفادة منها سواء في عرضها أو حفضها أو تحميلها.
4. اختتصارها للوقت والجهد وساعدت الباحثين في سرعة إنجاز بحوثهم وسرعة الاطلاع والحصول عليها.
5. توفرها بشكل مستمر دون تحديد لأوقات تواجدها أو انقطاعها.

ويرى الدباس (2010) أن توجه المكتبات نحو استخدام المصادر الإلكترونية بالإضافة إلى ما لديها من مصادر تقليدية له الكثير من الفوائد منها:

1- الاستفادة من مجموعة كبيرة من المعلومات في موضوع أو أكثر من خلال البحث المباشر للاستفادة من بنوك المعلومات وقواعد البيانات، فشبكات الاتصالات وفرت قدرة الربط مع أنظمة متعددة.
2- الاقتصاد في النفقات والتكاليف، مثل الاقتصاد في نفقات اشتراكات الدوريات الورقية وشراء الكتب، والتوفير في المبالغ التي تصرف على التزويد وأجور النقل ونفقات الإجراءات الفنية.

3- التغلب على مشكلة الحيز المكاني من خلال هذه المصادر.

4- فتح مجالات واسعة أمام المستفيدين من خلال البحث في قواعد البيانات، فهذا التنوع والسرعة والدقة ينعكس إيجابيا على المكتبة وخدماتها.

5- لقد غيرت المصادر الإلكترونية من بعض أدوار الموظفين في المكتبة، فقد حولت أمين المراجع التقليدية إلى أخصائي معلومات يشارك ويرشد المستفيد في الحصول على المعلومات من خلال البحث في قواعد البيانات أو القواعد المتاحة، فهذا ساهم بتغيير النظرة للخدمة المكتبية.

تقسيمات مصادر المعلومات الإلكترونية

يمكن تقسيم المصادر الالكترونية إلى: (عليان، 2010)

1. حسب نوعية الأوعية: هي النمط أو الأسلوب المقدم به المحتوى

أ. الكتب الإلكترونية: وهي الكتب التي تم إعدادها أو كتابتها باستخدام الحاسب الآلي أو تم تحويلها من الشكل المطبوع إلى الشكل الرقمي (المقروءة آلياً).

ب. الدوريات الإلكترونية: وهي نموذج مصور متاح على أحد مواقع شبكة الإنترنت اعتماداً على نظيره المطبوع، فمنها ما هو على أقراص مليزرة، ومنها ما هو متاح على الإنترنت من خلال الويب أو عبر البريد الإلكتروني سواء كان له إصدار ورقي أو الكترونيا فقط.

ج. المراجع الالكترونية: وهي الخدمات المرجعية المتوافرة عبر شبكة الإنترنت، وعادة ما تقدم بواسطة البريد الإلكتروني والرسائل الفورية، أو هي مجموعة من نماذج الأسئلة المعتمدة المتاحة على أحد مواقع شبكة الإنترنت، ويجيب عنها قسم المراجع في المكتبة بمفرده أو من خلال نظام تجميعي خدمة نقطة تساؤل ويتولى مسؤوليتها الأعضاء المشاركون في شبكة المراجع الكونية.

د. الرسائل الأكاديمية الإلكترونية: هي رسائل الماجستير والدكتوراة المتاحة في شكل الكتروني أكثر من إتاحتها في شكل ورقي، وتقابلها تلك المتاحة على نسخة ورقية إلى أن يتم تحويلها إلى شكل مقروء آلياً بواسطة الماسح الضوئي.

2. حسب الاستخدام أو التطبيق: ووفق هذا المعيار يمكن أن تنقسم المصادر الالكترونية إلى:

أ. الملفات الببليوغرافية: وهي تلك التي تتضمن بيانات ببليوغرافية تحيل المستفيد إلى مصادر المعلومات ومن ثم فهي تقوم بدور أدوات البحث عن اوعية المعلومات مثل الفهارس وغيرها.

ب. ملفات النص الكامل العددية والرسومية: ويمكن أن تتضمن الصفحات الخاصة المتاحة على شبكة الإنترنت سواء الخاصة بأحد الأفراد أم المؤسسات أم التي تتناول أحد الموضوعات.

ج. برامج إعادة النماذج والإرشادات: وتعطي هذه البرامج تعليمات وإرشادات للمستفيد عبر سلسلة من المفاهيم والعمليات والنماذج التي غالباً ما تكون تفاعلية عند تعامل المستفيد معها، كما أنها عادة ما تتضمن نصوصاً للتعليم المبرمج وبرامج المحاكاة والنمذجة.

د. برامج التطبيقات: وهي البرامج التي يتم من خلالها إجراء أحد التطبيقات على الحاسب الآلي، من خلال إدخال ومعالجة بيانات نصية أو عددية.

3. حسب طرق الإتاحة والوصول: وتتمثل في محطات العمل المستقلة، والشبكات المحلية، والشبكات المحلية المتاحة عن بعد، والفهارس المتاحة على الخط المباشر، وشبكة الإنترنت.

وأشار المصري (2015) إلى عدة طرق للحصول على مصادر المعلومات الإلكترونية وهي:

1. الاتصال بقواعد البيانات من خلال الاتصال المباشر.
2. شراء حق الإفادة من الخط المباشر.
3. الاشتراك في الشبكات المحلية والإقليمية والدولية.
4. الاشتراك في شبكات تعاونية خاصة لتقاسم مصادر المعلومات.
5. الاشتراك من خلال وسطاء المعلومات أو تجار المعلومات.
6. من خلال شبكة الإنترنت.

المكتبات الرقمية

وهي مجموعة المصادر الإلكترونية والإمكانات الفنية ذات العلاقة بإنتاج المعلومات والبحث عنها، فهي امتداد ودعم لنظم خزن واسترجاع المعلومات (بو عزة، 2006).

وأشار عليان (2010) إلى أن الهدف الشامل للمكتبة الرقمية يتمثل بالعمل على تطوير طرق جمع وخزن وتنظيم واستخدام مختلف مصادر المعلومات الإلكترونية عبر مختلف منافذ الوصول وقنوات الوصول الإلكترونية لإشباع الاحتياجات المعلوماتية، كذلك تهدف إلى:

1. المشاركة والإسهام في إنتاج المعرفة وتقاسمها والإفادة منها.
2. مساعدة مؤسسات البحث العلمي والهيئات التعليمية، ويتمثل ذلك في إدارة المصادر الرقمية والنشر الإلكتروني وغيرها من الأنشطة.
3. المساهمة بتوزيع وإيصال المعلومات إلى المجتمع بشكل أسرع وأقل تكلفة، وذلك عبر مختلف منافذ وقنوات الوصول الإلكترونية لتوفير مختلف الاحتياجات المعلوماتية.

4. جمع وتخزين وتنظيم المعلومات وذلك بأشكال رقمية.
5. التعاون بين مؤسسات البحث العلمي والهيئات التعليمية والتجارية.
6. المساهمة بإحداث تطورات مذهلة وذلك على صعيد تخزين البيانات واسترجاع المعلومات.
7. المحافظة على مصادر المعلومات النادرة والسريعة التلف دون حجب الوصول إليها من جانب الراغبين في دراستها والاطلاع عليها.
8. توفر المكتبة الرقمية للمستفيدين أدوات للتعامل مع المعلومات أكثر فاعلية من الأدوات التقليدية من حيث التخزين والحفظ السريع والأرشفة والبحث.
9. فتح آفاق جديدة في التفاعل مع الآخرين، حيث يمكن للقارئ مشاهدة تعليقات القراء الآخرين للكتاب ومشاهدة تقييمهم له وأحياناً الدخول في مناقشة حية أو عن طريق الرسائل وغيرها.
10. إصدار النشرات بشكل يومي من خلال موقعها على شبكة الإنترنت دون تكاليف كبيرة.
11. تستطيع نشر كشافاتها ومستخلصاتها ونظم استرجاع المعلومات ومن ثم يستطيع المستفيد الحصول عليها من أي مكان بكل سهولة ويسر.

وأشار بو عزة (2006) إلى أبرز وظائف المكتبة الرقمية وهي:

1. وظيفة الانتقاء واقتناء موارد معلومات من شبكة الويب: فالوظيف التقليدية في اقتناء أوعية المعلومات تكون حسب حاجات المستفيدين، إلا أنه مع ظهور الإنترنت طرحت مشكلة كيفية التعرف على الجمهور واختيار المواد المناسبة له؛ فهو غير معروف بشكل جيد، لذا لابد من اجراء دراسات ميدانية للتعرف الى المستفيدين، وبتعويض مصادر رقمية بالمصادر التقليدية.
2. وظيفة فهرسة المصادر: تقوم المكتبات الرقمية بفهرسة المصادر ووضعها في روابط.
3. وظيفة الاتصال وإدارة حقوق الملكية: تهتم المكتبات الرقمية بحقوق الوصول إلى المصادر الرقمية التي تتيحها مؤسسات المعلومات وتوقيع عقود مع الناشرين والموزعين.
4. إنتاج الموارد الإلكترونية وإتاحتها: فالمكتبة تقوم برقمنة الأوعية الورقية مثل الرسائل الجامعية وغيرها، فيكون مختص المعلومات قام بالنشر مراعياً حقوق الملكية الفكرية بكل وثيقة.
5. حفظ الموارد الرقمية: وذلك لتفادي بعض المخاطر التي تتعرض لها وتتسبب في ضياعها فالأوعية الرقمية باتت تتأثر بالتطور التقني للتجهيزات الإلكترونية، ونتج عن ذلك أن بعض النصوص من الممكن أن تختفي بسبب تغيير الترميز وظهور معايير جديدة للتعرف إلى الرموز.

دوائر المعلومات في المكتبات الجامعية الأردنية

إن مكتبات الجامعات الأردنية في ظل سعيها لمواكبة تكنولوجيا المعلومات والاتصالات قامت باستحداث نظم وشبكات معلومات وآليات عمل جديدة للتحكم والسيطرة وتخزين وبث

المعلومات وتوفير أفضل السبل لقنوات الاتصال مع مختلف فئات المستفيدين ودخول مجتمع المعلومات من خلال تجهيز البنية التحتية اللازمة وتجهيزات حاسوبية وبرمجيات ومصادر معلومات إلكترونية، وذلك لما له من مردود علمي وثقافي وفوائد علمية وبحثية أكبر من الجهود والأموال المصروفة لتحقيق هذه الغاية، وكان لا بد من استحداث دوائر أو أقسام تشرف على هذه الأنظمة والشبكات والأجهزة التي توفرها هذه المكتبات، وتتابع عملها وتأمين الأمن والحماية لها والوقوف على المشاكل والصعوبات التي تتعلق بها وحلها بأفضل الطرق، والتعاون مع مراكز الحاسوب في الجامعات، وتزويد هذه الدوائر بالكوادر البشرية ذات الخبرة والكفاءة العالية في التعامل مع المحيط الإلكتروني الجديد، ومع أنها أحيانا قد تختلف في مسمياتها حسب الهيكل التنظيمي لهذه المكتبات مثل دائرة المعلومات ودائرة الخدمات الإلكترونية أو دائرة الدعم الفني أو قسم تطبيقات الحاسوب، إلا أنها تلتقي في تقديم الخدمات والمهمات والواجبات ذاتها، كما هو الحال في المثالين التاليين:

مثال1: دائرة المعلومات في مكتبة الجامعة الأردنية

في ظل الدور الكبير الذي تقوم به المكتبة الجامعية، فقد أولت الجامعة الأردنية اهتماما كبيرا بمكتبتها منذ تأسيسها وهيأت لها كافة الظروف لتكون متميزة في الأردن والعالم العربي. ويتمثل الهيكل التنظيمي للمكتبة من ثلاث دوائر رئيسة؛ من بينها دائرة المعلومات التي استحدثت في عام 1995. وتضم حاليا الشعب التالية، وهي: (مكتبة الجامعة الأردنية، 2016)

1. شعبة تطبيقات الحاسوب : تقوم هذه الشعبة بالإشراف على أجهزة الحاسوب، وتقم أيضا بأعمال البرمجة التي تحتاجها المكتبة، مثل برمجة المواقع الخاصة بالمكتبة والبرمجيات الأخرى التي تحتاجها المكتبة، بالإضافة إلى الإشراف على نظام الأفق وتصميم وتعديل موقع المكتبة ونسخ الأقراص المرافقة لمواد المكتبة، وعمل الباركود لجميع مواد المكتبة، وتقوم بتنفيذ مشروع لأرشفة الرسائل الجامعية إلكترونيا. وأشار الصلاح (2006) إلى أن هذه الشعبة أدت دور ضابط الارتباط بين المكتبة ومركز الحاسوب بالجامعة، وقد ساعدت هذه الشعبة على ما يلي:

- بناء نظام آلي لأتمتة العمليات المكتبية وإدارتها.
- مراقبة عمل الشاشات المنتشرة في قاعة الفهارس وإرشاد الطلبة لكيفية استخدامها.
- تدريب موظفي المكتبة على كيفية استخدام نظام الأفق في مختلف الشعب.
- مراقبة هذا النظام لمعرفة مواطن الضعف، وذلك بالتعاون مع مركز الحاسوب في الجامعة.
- دراسة احتياجات المكتبة من أجهزة الحاسوب والتوصية باقتناء المناسب منها.

- تولت مهمة مراقبة تمديد الكوابل الخاصة بأجهزة الحاسوب وتحديد النقاط الواجب توافر الحاسوب فيها.
- مراقبة برامج المكتبة الموزعة على الشعب المختلفة ومحاولة تحسينها.
- تدريب طلبة علم المكتبات والمعلومات في الجامعات والكليات الأردنية.

2. شعبة قواعد البيانات: تقوم هذه الشعبة بتوفير اشتراكات بقواعد البيانات الإلكترونية وتتيحها على الموقع الإلكتروني، وذلك بما يتناسب مع حاجة الكليات في الجامعة، وتقوم أيضا بتوفير الدوريات والصحف الورقية من خلال الشراء أو الإهداء.
3. شعبة الأرشفة والمصغرات الفيلمية: تقوم هذه الشعبة بمشروع لأرشفة الصحف والوثائق إلكترونيا وتقديم خدمات الاستنساخ لكافة المستفيدين.

مثال2: قسم قواعد البيانات والخدمات الإعلامية في مكتبة جامعة فيلادلفيا

يتولى هذا القسم الإشراف على تشغيل وإدارة برنامج الحاسب الآلي المستخدم والعمل على تطويره، والإشراف على أجهزة الحاسب الآلي ومركز المواد السمعية والبصرية والطابعات، والعمل على تطويرها وصيانتها بشكل دوري. ويقوم أيضاً بتدريب موظفي المكتبة على الخدمات المكتبية المحوسبة واستخدام شبكة الإنترنت واستخراج المعلومات من قواعد البيانات المختلفة، والإشراف على تدريب الطلبة وتمكينهم من استخدام أنظمة وبرامج الحاسب الآلي. ويهتم باستقبال الأسئلة والإستفسارات التي ترد المكتبة والرد عليها بالطرق التقليدية أو باستخدام الهاتف أو البريد الإلكتروني.

ثانياً: الدراسات السابقة:

أسفر البحث في الإنتاج الفكري المنشور حول موضوع أمن المعلومات في المكتبات الجامعية عن وجود عدد من الأبحاث والدراسات العربية والأجنبية، وقد جرى استعراض هذه الدراسات مصنفة وفق مستويين: الأول: الدراسات العربية، والثاني: الدراسات الأجنبية، مرتبة من الأقدم إلى الأحدث.

1. الدراسات العربية:

أجرى السريحي (2002) دراسة هدفت إلى إبراز موضوع أمن وسلامة المكتبات وتقنياتها والعاملين والمستفيدين من خلال دراسة حالة مكتبة جامعة الملك عبد العزيز بجدة. واعتمدت الدراسة على أسلوب المقابلة، وتكون مجتمع الدراسة من المسؤولين عن الجوانب الإدارية والتقنية في المكتبة، وأظهرت النتائج أن المكتبات ونظم المعلومات خاصة تتعرض لمخاطر تتعلق بالأمن والسلامة، وأن الحلول المطروحة للحفاظ على أمن المكتبات ممكنة عبر تطويع التقنيات الحديثة ووضع سياسات مناسبة، وأن مكتبة جامعة الملك عبد العزيز تعاني مجموعاتها المكتبية من عدم المتابعة الجيدة مما يعرضها للمخاطر الأمنية، ووجود عيوب بسياسات المكتبة المكتوبة، ولا يوجد فريق مختص يشرف على النظم الآلية في المكتبة، وأظهرت أيضا أن مبنى المكتبة الجديد لا يعاني من المشاكل التي كان يعاني المبنى القديم منها المتمثلة بتسرب المياه من السقف، وتقادم التسليك االكهربائي والتمديدات.

وأجرت با مفلح (2003) دراسة هدفت إلى قياس مدى كفاية الإجراءات الأمنية في شبكة مكتبات جامعة أم القرى، واعتمدت الدراسة على أسلوب المقابلة ، وتكون مجتمع الدراسة من مدير المكتبة والعاملين في قسم الحاسب الآلي، والمسئولين عن الشبكات في مركز المعلومات والحاسب الآلي بالجامعة. وأظهرت النتائج أن عمادة شؤون المكتبات تهتم بتطبيق أساليب متنوعة لحماية أمن المعلومات على شبكتها الخاصة بها تتمثل في: تأمين الناحية المادية بإتباع إجراءات خاصة بالمكان والتمديدات. ولكنها تفتقد بعض أساليب الحماية الضرورية، مثل الجدران النارية ودعم أجهزة عدم انقطاع التيار الكهربائي ونظام التشفير، وأن هناك بعض الجوانب السلبية في تطبيق أساليب الحماية المتبعة مثل، عدم تحديث برامج للحماية من الفيروسات بشكل منتظم، وتباعد الفترة بين كل نسخ احتياطي والنسخ التالي، وعدم تدريب الموظفين على بعض المشاكل التي تتعلق بأمن المعلومات وعدم مراعاة القواعد المتبعة لحماية كلمة المرور.

وأجرى الهادي (2006) دراسة نظرية هدفت للتعرف على واقع أمن وشفافية المعلومات في ظل الحكومة الإلكترونية. ناقشت الدراسة متطلبات الأمن الطبيعي لنظم المعلومات وبعض الأبعاد والاعتبارات المتعلقة بأمن المعلومات، وقدمت معايير أمن وشفافية المعلومات، وطرق

تنفيذ أمن المعلومات، وأوصت الدراسة بضرورة إقامة أطر سياسية وتنظيمية وقانونية لمواجهة مخاطر الأمن المعلوماتي، وتطوير سياسة أمن المعلومات وتطويعها لبرامج الحكومة الإلكترونية، ونشر الوعي بأهمية أمن المعلومات، وضرورة حماية نظم المعلومات.

وأجرى الزهيمي (2010) دراسة هدفت إلى التعرف على واقع أمن نظم المعلومات في المكتبات العمانية والتركيز على المكتبة الرئيسية بجامعة السلطان قابوس كونها تشكل نموذجاً للمكتبات العمانية، وتكون مجتمع الدراسة من المعنيين بالأنظمة الآلية بالمكتبة الرئيسية وفي مركز نظم المعلومات بجامعة السلطان قابوس. وأظهرت نتائج الدراسة انعدام المركزية في الإشراف الأمني على الأنظمة الآلية في المكتبة، وضعفا في شمولية إجراءات الحماية المتبعة بالمكتبة، وأن مركز نظم المعلومات بالجامعة يتبّع سياسة واضحة للتعامل لمواجهة بعض المخاطر المتوقعة مثل الاختراق وضياع أو تلف قاعدة البيانات، ولا تتوفر إجراءات للتعامل مع بعض التهديدات المتوقعة، مثل الانقطاع المفاجئ للكهرباء، وتعاني المكتبة من مشاكل تتعلق بسلامة البيانات في نظامها الآلي (سيمفوني)، وأنه لا توجد للمكتبة سياسة مكتوبة لإجراءات سلامة وأمن أنظمتها الآلية.

وأجرى عمار (2011) دراسة هدفت إلى تحديد وسائل وإجراءات حماية الشبكات الرئيسية ومصادر المعلومات الموجودة فيها أو المنقولة عنها والتحقق من صحة ضياعها، وتكون مجتمع الدراسة من العاملين في شبكات الحاسب الآلي وحمايتها ومديري الأقسام ومراكز المعلومات في المؤسسات التعليمية الحكومية والخاصة في مدينة الرياض، وتكون أفراد العينة من (105)، مكونيين من مهندسين وإداريين وفنيين يعملون في إدارة وتشغيل أجهزة وبرمجيات حماية شبكات الحاسب الآلي. وأظهرت نتائج الدراسة أن المؤسسات التي تعتمد على تقنية المعلومات في تسيير أعمالها توفر أجهزة لحماية شبكاتها مثل وسيط (Proxy) وجدران حماية. وتوفر المؤسسات موزعات مركزية ونقاط شبكة لا سلكية ونظم مكافحة الفيروسات ومراقبة استخدام الإنترنت، ويوجد لدى نصف المؤسسات مخططات واضحة لجدران الحماية والخوادم والموجهات وتحدث دوريا، ولا يتوفر في هذه المؤسسات نظام متكامل مخصص لإدارة قضايا أمن المعلومات، وكانت نقاط الضعف التي يمكن من خلالها أن تخترق الشبكات تتمثل في عدم تحديث أنظمة تشغيل جدران الحماية بانتظام والأداء الضعيف لبعض الأجهزة التي لا تستطيع مكافحة الفيروسات وقلة الخبرة بأمن المعلومات لدى العاملين وقلة الكفاية المهنية لدى المستخدمين وعدم وجود سياسة لحماية المعلومات. وأوصت الدراسة بضرورة وجود متخصصين في أمن المعلومات لإنشاء سياسة أمنية ومراجعتها وتدريب العاملين في الحماية لمساعدتهم بتأدية واجبهم

بشكل أمثل، وتوفير اجراءات العمل الخاصة بتقنية المعلومات وزيادة دخل الموظفين المسؤولين عن الحماية.

وأجرى اللوزي (2010) دراسة هدفت إلى التعرف على آراء العاملين في أجهزة الخدمة المدنية في الأردن عن الصعوبات التي تواجه تطبيق الخدمات الإلكترونية وتشمل البنية التحتية والتشريعات والسياسات التنظيمية وأمن المعلومات وسريتها والموارد المادية والإدارة والوعي الاجتماعي، وتم استخدام الاستبانة لجمع البيانات لعينة الدراسة التي تكونت من (413) موظفاً عاماً تم اختيارهم بطريقة عشوائية. وبينت النتائج أن اتجاهات المبحوثين تشير إلى اعتبار الإدارة من أهم الصعوبات التي تواجه تطبيق الخدمات الإلكترونية، ثم مجال الموارد المالية، ثم التشريعات والسياسات التنظيمية، ثم أمن المعلومات وسريتها، ثم الوعي الاجتماعي، وفي المرتبة الأخيرة مجال البنية التحتية. وبينت أيضا عدم وجود فروق ذات دلالة إحصائية بين آراء العاملين في الصعوبات التي تواجه تطبيق الخدمات الإلكترونية تعزى لمتغير الجنس والمؤهل العلمي والخبرة، بينما هناك فروق دالة تعزى لمتغير العمر وطبيعة العمل. وأوصت الدراسة بضرورة الاهتمام بإعداد العنصر البشري والإداري في أجهزة الحكومة وتحسين البنية التحتية والبيئة التشريعية للخدمات الإلكترونية في الأردن

أجرى العربي (2013) دراسة وصفية تحليلية هدفت إلى تحليل معايير (27002) لإدارة أنظمة أمن المعلومات الصادرة عن المنظمة الدولية للتوحيد القياسي (آيزو)، والتعرف على السياسات والتوجهات التي تتضمنها المعايير ومدى التزام أفضل الجامعات العربية بها،واعتمدت الدراسة الدراسة على المنهج الوصفي بالإضافة إلى منهج تحليل المضمون، وتكونت عينة الدراسة من أفضل (20) جامعة عربية حسب تصنيف ويبو متركس لتقييم الجامعات والمعاهد. وأظهرت النتائج أن جميع الجامعات التي شملتها الدراسة حرصت على تطبيق (11) معيارا أساسيا من معايير آيزو لإدارة أنظمة أمن المعلومات وجاءت في المرتبة الأولى جامعة الملك عبد العزيز بتطبيق (95) معياراً بنسبة 71.43% ، ثم جامعة الملك فهد بنسبة 58,65%، ثم جامعة أم القرى بنسبة 52,62%، الجامعة الأردنية بنسبة 51,88%. وأظهرت أن 80,95% من الجامعات موضوع الدراسة لم تحقق 50% من المعايير الفرعية. وأوصت بضرورة تطوير سياسة أمن المعلومات بالجامعات العربية وتحديد مهمات ومسؤوليات وحدات الجامعة فيما يخص تطبيق بنود سياسة أمن المعلومات، وضرورة توفير قدر عال من التدريب على إجراءات أمن المعلومات والتأكيد على امتلاك نسخ احتياطية من البيانات.

وأجرى الدنف (2013) دراسة هدفت إلى التعرف على واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة. وتكون مجتمع الدراسة من من 180 موظف في الكليات التقنية العاملين على نظم المعلومات في الكليات التقنية، وأظهرت نتائج الدراسة أن البنى التحتية لنظم المعلومات متوفرة بدرجة متوسطة، ولا توجد سياسات أمن معلومات واضحة في الكليات التقنية، وتتفاوت الكليات التقنية في درجة استخدام تعهد نظم المعلومات، وتوجد فروق إحصائية في آراء عينة الدراسة حول واقع أمن نظم المعلومات في الكليات التقنية.

2. الدراسات الأجنبية:

أجرى فيليبس PHELPS (2005) دراسة هدفت إلى قياس الكفاءة الذاتية لنظام أمن المعلومات في مكتبات فلوريدا. وبحثت العلاقة بين الجاهزية التعليمية لموظفي المكتبات (المكتبيين) في قسم النظام وفعالية تطبيق نظام أمن المعلومات لديهم. وقد عملت الدراسة على بحث العلاقة بين التدريب على تكنولوجيا المعلومات وفعالية امن نظام المعلومات عبر المتغيرات الوسيطة لتجربة أمن نظام المعلومات والكفاءة الذاتية لنظام المعلومات وإطلاق مهمة أمن نظام المعلومات واستمرارية مهمة أمن نظام المعلومات. كان المشاركون في هذه الدراسة من الموظفين في مكتبات فلوريدا الأكاديمية والعامة. وقد تم الحصول على 56 إجابة قابلة للاستخدام. وقد وجدت الدراسة أن المكتبيين ذوي التدريب السابق في تكنولوجيا المعلومات كانوا أكثر فعالية في تطبيق أمن نظام المعلومات مقارنة بمن لم يحصلوا على التدريب. ورغم عدم تقديم الدراسة الدعم للنموذج بشكل كامل، فقد أظهرت النتائج وجود علاقات هامة بين وجود التدريب السابق في مجال أمن نظم المعلومات، والكفاءة الذاتية لنظام المعلومات وفعالية تطبيق نظام أمن المعلومات. واظهر الجنس ارتباطاً ضعيفا بين المتغيرين، ولكن تحليلات الانحدار قد أظهرت عدم وجود إمكانية تنبؤ. خبرة العمل كانت عامل تنبؤ أفضل بالفعالية من التدريب على تكنولوجيا المعلومات، ولكن ليس بقوة كفاءة الذات. وأوصت الدراسة بضرورة تدريب موظفي المكتبات وإكسابهم الخبرات المطلوبة فيما يتعلق بأمن نظم المعلومات.

أجرى مايدبيونو وأوانج Maidabino &Awang (2011) دراسة هدفت إلى تقييم إدارة أمن المكتبات الجامعية، وتكونت عينة الدراسة من 60 موظفاً في في 4 من المكتبات الجامعية في نيجيريا. وأظهرت النتائج عدم وجود سياسات وخط لأمن المعلومات في هذه المكتبات، وضعف بعض إجراءات الأمن المادي مثل عدم وجود أجهزة إنذار لمنع السرقة، وهناك ضعف في الوعي الأمني لدى الموظفين. وقد أوصت الدراسة بأن الحاجة إلى موظفين

ومستخدمين واعين في المكتبات هو أمر مهم لأمن المجموعة العامة. وينبغي أن يكون الموظفون والمستخدمون لديهم المعرفة الكافية بأهمية عمل أمن المجموعات المكتبية لأن قلة الوعي قد يؤدي إلى خرق مقصود أو غير متعمد لأمن المجموعة، وهناك حاجة إلى زيادة الأمن في مقر المكتبة من خلال الإشراف والمراقبة، وينبغي وضع سياسات وإجراءات وتنفيذها ويجب أن تكتب مثل هذه السياسات وترسل إلى كل من الموظفين والمستخدمين للاطلاع عليها وتنفيذها .

وقام أوسياندي Osayandy (2011) بدراسة هدفت إلى الكشف عن أنظمة الأمن الإلكترونية في المكتبات الأكاديمية في ثلاث جامعات في جنوب غرب نيجيريا. وتكونت عينة الدراسة من (109) من أمناء المكتبات الجامعية ، ورؤساء أقسام الخدمات الفنية، وغيرهم من الموظفين في المكتبات الأكاديمية في ثلاث جامعات (كوفنانت، وبابكوك، ولاغوس) استجاب مهم (81). أظهرت نتائج الدراسة أن المكتبات الأكاديمية تعاني من القضايا الأمنية، لذلك فهي بحاجة إلى تحسين الأجهزة الأمنية للمحافظة على أنظمة معلومات المكتبات، كما أشارت نتائج الدراسة إلى أن الجامعات الثلاثة لديها نظاما إلكترونيا مثبتا في مكتباتها، وأكد أفراد عينة الدراسة في جامعة بابكوك أن كاميرات المراقبة في المكتبة تعمل بشكل فعال، كما أكد أفراد عينة الدراسة في جامعتي كوفنانت لاغوس على أن الكاميرات المثبتة على بوابات الأنظمة الأمنية تعمل بشكل فعال، وهذا يعني أن الجامعات الثلاثة تستخدم نظام أمني إلكتروني مثبت في مكتباتها، كما بينت النتائج وجود طرق مختلفة يتم بها أخذ المواد المكتبية بشكل غير قانوني.

أجرت إسماعيل وأوانج Ismail &Awang (2011) دراسة في ماليزيا هدفت إلى التعرف على أمن أنظمة المعلومات في المكتبات العامة والخاصة. وتكونت عينة الدراسة من (50) من الأفراد المسؤولين عن أمن أنظمة المعلومات في المكتبات الخاصة والعامة في ماليزيا، وأظهرت نتائج الدراسة أن (95%) من المكتبات ذات مستوى مرتفع في تحقيق الأمن الإلكتروني لأنظمة معلومات المكتبات، كما أشارت النتائج إلى أن (54%) من المكتبات كانت تعاني من سوء التدابير التنظيمية، مثل: عدم وجود إجراءات الأمن المناسبة، وعدم توفير الأدوات الإدارية التي من شأنها أن تساعد على أمن أنظمة المعلومات، بالإضافة إلى قلة الأنشطة التوعوية، وقد يعود ذلك إلى الإفراط في التركيز على التكنولوجيا باعتبارها الحل الوحيد لكافة الأجهزة الأمنية.

وأجرت إسماعيل Ismail (2012) دراسة هدفت إلى تقييم إدارة أمن المعلومات في المكتبات الأكاديمية الماليزية. وتكونت عينة الدراسة من(39) من الأفراد المسؤولين عن نظم المعلومات أو تكنولوجيا المعلومات في المكتبات الأكاديمية الماليزية ووضع خمسة معايير لتقييم الأمن شملت التدابير التكنولوجية وسياسات أمن المعلومات والإجراءات الأمنية ووسائل الأمن وأنشطة التوعية الأمنية، وأظهرت النتائج أن أكثر التهديدات الأمنية شيوعا في المكتبات

الأكاديمية الماليزية هي تهديدات أمن الأجهزة وبنسبة (70.0%)، والمخاطر البشرية (66.0%)، والتهديدات البيئية (51.0%)، وأظهرت أيضا أن هناك أخطاء في صيانة الأجهزة واستخدام الأجهزة غير المصرح بها وتعرض أجهزة المكتبة للفيروسات، وأظهرت أن هناك فروقا بين المكتبات في تطبيق التدابير الأمنية في جوانب الميزانية وتوفر نظم المعلومات وعدد الموظفين. وأوصت بضرورة وضع تدابير تنظيمية في المكتبات لأن الاعتماد على التكنولوجيا وحدها لا يكفي في حل مشكلة أمن المعلومات بشكل فعال.

أجرى أكور Akor (2013) دراسة هدفت التعرف على الإدارة الأمنية للوقاية من سرقة الكتاب في المكتبات الجامعية من خلال دراسة حالة جامعة ولاية بينو في نيجيريا، وتكون مجتمع الدراسة من جميع العاملين في المكتبة وعددهم (48) استجاب منهم (30). وأظهرت النتائج أن الكتب في مكتبة الجامعة تتعرض للسرقة والتشويه بسبب عدم كفاية الإجراءات الأمنية وعدم كفاية المواد المكتبية والقيود المالية إلى جانب أنانية مستخدمي المكتبة، وأظهرت أيضا أن أساليب مختلفة اعتمدت لسرقة وتشويه الكتب تشمل تمزيق بعض صفحات الكتاب وإزالة صفحات الغلاف وإخفاء الكتب بالملابس. وأوصت بأنه ينبغي أن تتوفر خدمات التصوير ليتمكن مستخدمو المكتبة من تصوير المواد المكتبية التي هي قليلة وتوفير مواد كافية لتلبية احتياجاتهم.

التعقيب على الدراسات السابقة

يتضح من خلال عرض الدراسات السابقة ما يلي:

1. عدم وجود أي دراسة ميدانية تناولت موضوع أمن المعلومات في مكتبات الجامعات الأردنية حسب علم الباحث.
2. أن الدراسات التي اتفقت مع هذه الدراسة في موضوع أمن المعلومات في المكتبات الجامعية كانت دراسة السريحي (2001)، ودراسة با مفلح (2003)، ودراسة الزهيمي (2010)، ودراسة عمار (2010)، ودراسة فيليبس PHELPS (2005)، ودراسة مايدبيونو وأوانج Maidabino &Awang (2011)، ودراسة أوسياندي Osayandy (2011)، ودراسة إسماعيل وأوانج Ismail &Awang (2011)، ودراس إسماعيل Ismail (2012)، ودراسة أكور Akor (2013).
3. أنه لقلة الدراسات المباشرة حول موضوع أمن المعلومات في المكتبات الجامعية باللغة العربية، فقد اشتملت الدراسات السابقة على دراسات أخرى ذات علاقة بالموضوع حول أمن المعلومات في المؤسسات التعليمية مثل دراسة العربي (2013)، ودراسة الدنف (2013)،

ودراسات أخرى تناولت بعض الأبعاد والاعتبارات المتعلقة بأمن وشفافية المعلومات في ظل التطورات التكنولوجية مثل دراسة الهادي (2006)، ودراسة اللوزي (2010).

4. تختلف هذه الدراسة عن الدراسات السابقة في إطارها الزماني والمكاني.

ويمكن إجمال الأبعاد التي تم فيها الإفادة من الدراسات السابقة بلآتي:

1. تنظيم الدراسة بشكل عام.
2. بناء منهجية الدراسة.
3. إنشاء الاستبانة.
4. مناقشة النتائج والتوصيات.

الفصل الثالث

الطريقة والاجراءات

يتضمن هذا الفصل وصفا للإجراءات التي قام بها الباحث لتحقيق أهداف هذه الدراسة، والذي تضمن وصف مجتمع الدراسة والطريقة التي اختير بها، وكذلك وصف أداة الدراسة والإجراءات التي اتبعت للتأكد من صدقها وثباتها، وكيفية تطبيقها على أفراد العينة، ووصف طريقة جمع البيانات وأسلوب التصحيح، فضلاً عن الإشارة إلى الأساليب الإحصائية التي استخدمت، وذلك على النحو الآتي:

منهج الدراسة :

تقوم هذه الدراسة على استخدام المنهج الوصفي المسحي، وقد استخدم هذا المنهج لمناسبته لطبيعتها واستعراض أهم الأدبيات ذات العلاقة **"بواقع أمن المعلومات من وجهة نظر العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية والصعوبات التي يواجهونها"**.

مجتمع الدراسة:

تكون مجتمع الدراسة من جميع العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية الحكومية والخاصة، وعددهم 96 عاملاً (مديراً، ورئيس قسم، وموظفاً). ونظراً لصغر مجتمع الدراسة فإن عينة الدراسة هي مجتمعها، إذ تم توزيع (96) استبانة على المجتمع كاملاً، وبعد استرجاع الاستبانات تم استبعاد (12) استبانة لعدم صلاحيتها لأغراض التحليل الإحصائي بسبب عدم اكتمال الاستجابات، أو تسليم الأداة فارغة، أو بسبب عدم مشاركة بعض أفراد المجتمع بتعبئة أداة الدراسة، فتمثل مجتمع الدراسة بـ (84) عاملاً في مكتبات الجامعات الأردنية التي تمثل ما نسبته (87.5%) من العينة الرئيسة، والجدول رقم (1) يوضح توزيع أفراد مجتمع الدراسة حسب الخصائص الديموغرافية.

الجدول (1)

توزيع أفراد مجتمع الدراسة حسب المتغيرات الديموغرافية

المتغير	التكرار	النسبة المئوية
الخبرة		
5 سنوات فما دون	24	28.6

10-6 سنوات	24	28.6
أكثر من 11 سنة	36	42.9
المجموع	84	100.0
نوع الجامعة		
حكومية	44	52.4
خاصة	40	47.6
المجموع	84	100.0
المستوى الوظيفي		
مدير	3	3.6
رئيس قسم / شعبة	29	34.5
موظف	52	61.9
المجموع	84	100.0
التخصص		
هندسة حاسوب	---	---
مكتبات ومعلومات	36	42.9
علم الحاسوب	16	19.0
تخصص آخر	32	38.1
المجموع	84	100.0

أداة الدراسة:

تم تطوير (مقياس واقع أمن المعلومات من وجهة نظر العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية والصعوبات التي يواجهونها) بالرجوع إلى الأدب النظري والدراسات السابقة كدراسة بامفلح (2003)، ودراسة الدنف (2013)، ودراسة الزهيمي (2010)، ودراسة فيليبس (2005) Phelps، هذا وقد تكون مقياس الدراسة من ثلاثة أجزاء:

الجزء الأول: يتضمن المعلومات الديمغرافية، والمكونة من: الخبرة، ونوع الجامعة، والمستوى الوظيفي، والتخصص.

الجزء الثاني: يتضمن (49) فقرة، وجميعها تتعلق بأمن المعلومات من وجهة نظر العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية، وتم تقسيمها إلى خمسة محاور، هي:

المحور الأول: أمن البنية التحتية في المكتبات، ويتضمن الفقرات من 1-20، ويتفرع منه الأبعاد الآتية:

- البعد الأول، ويتناول الأمن المادي، ويتضمن الفقرات من (1-8).
- البعد الثاني المتعلق بحماية الأفراد، ويتضمن الفقرات من (9-12).
- البعد الثالث المتعلق بأمن البرمجية، ويتضمن الفقرات من (13-20).

- المحور الثاني: سياسة أمن المعلومات، ويتضمن الفقرات من (21-25).

- المحور الثالث: حماية البيانات الإلكترونية في المكتبة، ويتضمن الفقرات من (26-31).

- المحور الرابع: إجراءات حماية أنظمة وشبكات الحاسوب في المكتبة، ويتضمن الفقرات من (32-40).

- المحور الخامس: التحكم بالوصول لنظم المعلومات، ويتضمن الفقرات من (41-49)

الجزء الثالث: يتضمن (11) فقرة تتعلق بالصعوبات التي يواجهها العاملون بدوائر المعلومات في مكتبات الجامعات الأردنية.

وعليه فقد بلغ عدد فقرات الاستبانة بصيغتها النهائية (60) فقرة كما هي موضحة في الملحق رقم (1)، واستخدم فيها مقياس ليكرت الخماسي على الشكل التالي: (موافق بشدة، موافق، محايد، غير موافق، غير موافق بشدة)

صدق أداة الدراسة:

صدق المحتوى:

تم عرض المقياس الذي يتكون من (69) فقرة بعد إعداد الصورة الأولية على (13 محكماً) من أعضاء الهيئة التدريسية في قسم المكتبات وذوي الاختصاص في التخصصات الأخرى مثل (تكنولوجيا المعلومات)، ملحق (2)، وذلك لإبداء آرائهم في صدق المضمون وانتماء العبارات للمقياس ومدى ملاءمتها لقياس ما وضعت لقياسه، ودرجة وضوحها، ومن ثم تم اقتراح التعديلات المناسبة، وقد تم اعتماد معيار (80%) لبيان صلاحية الفقرة، وبناء على آراء المحكمين تم تعديل بعض الفقرات من ناحية الصياغة لزيادة وضوحها، وتم حذف (3) فقرات بسبب تشابهها وقرب مدلولها مع فقرات أخرى، وتم حذف (6) فقرات لعدم مناسبتها لأغراض الدراسة وعدم مناسبة بعضها للبعد الذي تنتمي إليه، وبالنتيجة أصبح المقياس يتألف من (60) فقرة موزعة على خمسة محاور رئيسة، بالإضافة إلى الصعوبات التي تواجه العاملين بدوائر المعلومات في المكتبة، ملحق (2)، واعتبر الباحث آراء المحكمين وتعديلاتهم دلالة على صدق

محتوى أداة الدراسة وملاءمة فقراتها وتنوعها، وبعد إجراء التعديلات المطلوبة، تحقق التوازن بين مضامين المقياس في فقراته، وقد عبر المحكمون عن رغبتهم في التفاعل مع فقراته، مما يشير للصدق الظاهري للأداة.

ثبات أداة الدراسة:

للتعرف إلى اتساق كل فقرة من المقياس مع البعد الذي تنتمي إليه الفقرة، قام الباحث باستخدام حساب معاملات الارتباط بين كل فقرة من الفقرات في المقياس عن طريق استخدام معامل (كرونباخ ألفا) ويبين الجدول (2) نتائج الاختبار:

جدول (2): معاملات الثبات لفقرات أداة الدراسة باستخدام اختبار كرونباخ ألفا)

متغيرات الدراسة	معامل الثبات باستخدام كرونباخ ألفا
الأمن المادي	0.79
حماية الأفراد	0.80
أمن البرمجية	0.84
سياسة أمن المعلومات	0.89
حماية البيانات الإلكترونية في المكتبة	0.90
إجراءات حماية أنظمة وشبكات الحاسوب في المكتبة	0.87
التحكم بالوصول لنظم المعلومات	0.89
الصعوبات التي تواجه العاملين بدوائر المعلومات في المكتبة	0.88
الأداة ككل	0.94

يتضح من الجدول (2) أن قيم معامل كرونباخ ألفا للمحاور الفرعية للمقياس تراوحت بين (0.79 – 0.90) وكما بلغت قيمة معامل الثبات باستخدام كرونباخ ألفا للدرجة الكلية للمقياس (0.94).

مفتاح تصحيح المقياس

تم مراعاة أن يتدرج مقياس ليكرت المستخدم في الدراسة تبعاً لقواعد وخصائص المقاييس كما في الجدول رقم (3):

جدول رقم (3): مقياس ليكرت

موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
5	4	3	2	1

واعتماداً على ما تقدم فإن قيم المتوسطات الحسابية التي توصلت إليها الدراسة تم التعامل معها على النحو الآتي وفقاً للمعادلة التالية:

القيمة العليا – القيمة الدنيا لبدائل الإجابة مقسومة على عدد المستويات، أي:

$\frac{(5-1)}{3} = \frac{4}{3} = 1.33$ وهذه القيمة تساوي طول الفئة.

وبذلك تكون المستويات كما في الجدول رقم (4):

الجدول رقم (4): مستويات الموافقة

المستوى	طول الفئة
المنخفض	2.33 - 1.00
المتوسط	3.67 - 2.34
المرتفع	5.00 - 3.68

إجراءات الدراسة:

مرت عملية إعداد أداة الدراسة بالخطوات التالية:

1- الاطلاع على الدراسات السابقة المتعلقة بموضوع الدراسة والمختصة بأمن المعلومات من وجهة نظر العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية و بعض أدوات القياس.

2- بناء محاور وفقرات المقياس بحيث يتماشى وأسئلة الدراسة.

3- تحكيم المقياس من قبل مجموعة من المحكمين المختصين وإجراء التعديلات المقترحة في ضوء ملاحظاتهم.

4- الحصول على كتاب تسهيل مهمة من إدارة الجامعة الأردنية موجه إلى الجامعات الأردنية وخصوصاً المكتبات المختصة بالدراسة، لتطبيق أداة الدراسة.
5- توزيع أداة الدراسة على أفراد مجتمع الدراسة (العاملين في بدوائر المعلومات في مكتبات الجامعات الأردنية)، وقد تم التطبيق من قبل الباحث بتوضيح بعض الجوانب المتعلقة بالدراسة وشرح أهدافها وأهميتها والتأكيد على سرية المعلومات واستخدامها لغرض البحث العلمي فقط، بالإضافة إلى التأكيد على ضرورة الجدية والدقة في التعامل مع أدوات القياس، كما تم اختيار الأماكن المناسبة للتطبيق، وبعد الانتهاء من التطبيق مباشرة تم جمع أداة الدراسة وفرزها واستبعاد ما هو غير صالح للتحليل الإحصائي.
6- بعد تحويل الاستجابات إلى درجات خام، تم إدخال البيانات إلى الحاسوب وإجراء المعالجات الإحصائية لها باستخدام برنامج الرزم الإحصائية (SPSS) وإجراء التحليلات الإحصائية المناسبة للإجابة عن أسئلة الدراسة واستخراج النتائج ومناقشتها.
7- استغرق زمن التطبيق الفردي (15) دقيقة. أما عملية جمع البيانات الكلية فقد استغرقت (20) يوماً.

متغيرات الدراسة:

اشتملت الدراسة على العديد من المتغيرات:

أولاً: المتغيرات المستقلة وتشمل:

أ- المتغيرات الديموغرافية:

1- الخبرة.
2- نوع الجامعة.
3- المستوى الوظيفي.
4- التخصص.

ثانياً: المتغير التابع: ويشمل استجابات أفراد مجتمع الدراسة عن أمن المعلومات من وجهة نظر العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية والصعوبات التي يواجهونها.

الأساليب الإحصائية المستخدمة:

تم استخدام أساليب الإحصاء الوصفي للإجابة عن أسئلة الدراسة، كالآتي:

- استخراج التكرارات والنسب المئوية لوصف أفراد عينة الدراسة.

- استخدام اختبار كرونباخ ألفا للتأكد من ثبات الأداة.
- للإجابة عن السؤالين الاول والثاني، تم حساب المتوسطات الحسابية والانحرافات المعيارية.
- للإجابة عن السؤالين الثالث والرابع تم استخدام تحليل التباين المتعدد Four Ways ANOVA.
- استخدام اختبار شيفيه للا البعدية في حالة وجود فروق دالة إحصائياً تبعاً لمتغيرات سنوات الخبرة، ونوع الجامعة، والمسمى الوظيفي، والتخصص.

الفصل الرابع

نتائج الدراسة

تمهيد:

يتضمن هذا الفصل الإجابة عن أسئلة الدراسة، حيث تم استخراج المتوسطات الحسابية والانحرافات المعيارية للتعرف إلى استجابات أفراد عينة الدراسة عن **" واقع أمن المعلومات من وجهة نظر العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية والصعوبات التي يواجهونها"**، وفيما يلي الإجابة عن أسئلة الدراسة التالية:

السؤال الأول : ما واقع أمن المعلومات من وجهة نظر العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية؟

للإجابة عن السؤال الأول، تم استخراج المتوسطات الحسابية والانحرافات المعيارية للتعرف إلى استجابات أفراد عينة الدراسة عن واقع أمن المعلومات من وجهة نظر العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية، والجدول (5) يوضح ذلك

الجدول (5)

المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة عن فقرات " واقع أمن المعلومات من وجهة نظر العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية " مرتبة ترتيباً تنازلياً

الرقم	المحور	المتوسط الحسابي	الانحراف المعياري	الترتيب	المستوى
4	إجراءات أنظمة وشبكات الحاسوب في المكتبة	3.73	0.64	1	مرتفع
5	التحكم بالوصول لنظم المعلومات	3.68	0.75	2	مرتفع
1	أمن البنية التحتية في المكتبات	3.61	0.62	3	متوسط
3	حماية البيانات الالكترونية في المكتبة	3.49	0.85	4	متوسط
2	سياسة أمن المعلومات	3.32	0.82	5	متوسط
	المتوسط العام الحسابي	3.57	0.62		متوسط

يتضح من الجدول رقم (5) أن المتوسطات الحسابية لـ (**واقع أمن المعلومات من وجهة نظر العاملين بدوائر المعلومات في مكتبات الجامعة الأردنية**)، تراوحت ما بين (3.32-3.73)، حيث حاز الواقع على متوسط حسابي إجمالي (3.57)، وهو من المستوى المتوسط، وقد حاز المحور رقم (4) على أعلى متوسط حسابي حيث بلغ (3.73)، وبانحراف معياري (0.64)، وهو من المستوى المرتفع، وقد تمثل المحور في (إجراءات أنظمة وشبكات الحاسوب في المكتبة)، وفي المرتبة الثانية جاء محور رقم (5) بمتوسط حسابي بلغ (3.68) وبانحراف معياري (0.75) وهو من المستوى المرتفع، حيث تمثل المحور في (التحكم بالوصول لنظم المعلومات).

وفي المرتبة الأخيرة محور رقم (2) بمتوسط حسابي (3.32) وبانحراف معياري (0.82)، وهو من المستوى المتوسط، حيث نص المحور على (سياسة أمن المعلومات).

وهذا يفسر أن واقع أمن المعلومات متوسط المستوى من وجهة نظر العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية.

وللتعرف إلى المتوسطات الحسابية والانحرافات المعيارية للفقرات الفرعية لكل محور من المحاور الفرعية لواقع أمن المعلومات، تم حساب المتوسطات الحسابية والانحرافات المعيارية، وفيما يلي هذه النتائج:

1- واقع أمن البنية التحتية في المكتبات

تم استخراج المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة للتعرف إلى مستوى أمن البنية التحتية في المكتبات من وجهة نظر العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية والمتمثل في كل من (الأمن المادي، وحماية الأفراد، وأمن البرمجية)، وفيما يلي هذه النتائج:

أ- واقع الأمن المادي:

تم استخراج المتوسطات الحسابية والانحرافات المعيارية للتعرف إلى مستوى واقع الأمن المادي بدوائر المعلومات في مكتبات الجامعات الأردنية، والجدول (6) يوضح ذلك:

الجدول (6)

المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة عن فقرات "واقع الأمن المادي في مكتبات الجامعات الأردنية" مرتبة ترتيباً تنازلياً

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	الترتيب	المستوى
4	يتوافر أجهزة لكشف الحريق والإنذار حالة حدوثه.	4.08	0.98	1	مرتفع
8	يمنع الموظف غير المختص من إجراء أي تعديل مادي على الأجهزة في المكتبة.	3.93	0.98	2	مرتفع
2	جميع كوابل الكهرباء والاتصالات التي تنقل البيانات محمية من العبث بها أو الإتلاف داخل المكتبة.	3.68	1.16	3	مرتفع
5	مداخل ومخارج المكتبة مؤمنة بأجهزة إنذار إلكترونية.	3.50	1.24	4	متوسط
7	هناك صيانة مستمرة للأجهزة بشكل يضمن استمرارية عملها.	3.48	1.08	5	متوسط
6	يتوافر بالمكتبة أجهزة تكييف وتهوية كافية.	3.38	1.23	6	متوسط
3	يتوافر وسائل تصريف للمياه ومضخات شفط عند الحاجة.	3.29	1.11	7	متوسط
1	يوجد مصدر احتياطي للكهرباء داخل المكتبة.	3.20	1.42	8	متوسط
	المتوسط العام الحسابي	3.57	0.74		متوسط

يتضح من الجدول (6) أن المتوسطات الحسابية لـ (**واقع الأمن المادي في مكتبات الجامعات الأردنية من وجهة نظر العاملين بدوائر المعلومات**)، تراوحت ما بين (3.20-4.08)، حيث حاز الواقع على متوسط حسابي إجمالي (3.57)، وهو من المستوى المتوسط، وقد حازت الفقرة رقم (4) على أعلى متوسط حسابي حيث بلغ (4.08)، وبانحراف معياري (0.98)، وهو من المستوى المرتفع، وقد نصت الفقرة على (يتوافر أجهزة لكشف الحريق والإنذار حالة حدوثه)، وفي المرتبة الثانية جاءت الفقرة رقم (8) بمتوسط حسابي بلغ (3.93) وبانحراف معياري (0.98) وهو من المستوى المرتفع، حيث نصت الفقرة على (يمنع الموظف غير المختص من إجراء أي تعديل مادي على الأجهزة في المكتبة).

وفي المرتبة الأخيرة جاءت الفقرة رقم (1) بمتوسط حسابي (3.20) وبانحراف معياري (1.42)، وهو من المستوى المتوسط، حيث نصت الفقرة على (يوجد مصدر احتياطي للكهرباء داخل المكتبة).

ب-واقع حماية الأفراد:

تم استخراج المتوسطات الحسابية والانحرافات المعيارية للتعرف إلى مستوى واقع حماية الأفراد بدوائر المعلومات في مكتبات الجامعات الأردنية، والجدول (7) يوضح ذلك:

الجدول (7)

المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة عن فقرات "واقع حماية الأفراد في مكتبات الجامعات الأردنية" مرتبة ترتيباً تنازلياً

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	الترتيب	المستوى
12	يتم محاسبة الموظف الذي ينتهك إجراءات أمن المعلومات داخل المكتبة.	3.83	0.94	1	مرتفع
11	يشترط على الموظفين عدم إفشاء إجراءات الأمن والرقابة.	3.69	0.88	2	مرتفع
10	يتم تحديد مسؤوليات الموظف ومهماته تجاه أمن المعلومات في المكتبة.	3.54	0.99	3	متوسط
9	يتم متابعة المستخدمين وتسجيل الحوادث التي تخص أمن المعلومات داخل المكتبة.	3.48	1.06	4	متوسط
	المتوسط العام الحسابي	3.63	0.76		متوسط

يتضح من الجدول (7) أن المتوسطات الحسابية لـ (**واقع حماية الأفراد في مكتبات الجامعات الأردنية من وجهة نظر العاملين بدوائر المعلومات**)، تراوحت ما بين (3.48-3.83)، حيث حاز الواقع على متوسط حسابي إجمالي (3.63)، وهو من المستوى المتوسط، وقد حازت الفقرة رقم (12) على أعلى متوسط حسابي حيث بلغ (3.83)، وبانحراف معياري (0.94)، وهو من المستوى المرتفع، وقد نصت الفقرة على (يتم محاسبة الموظف الذي ينتهك إجراءات أمن المعلومات داخل المكتبة)، وفي المرتبة الثانية جاءت الفقرة رقم (11) بمتوسط حسابي بلغ (3.69) وبانحراف معياري (0.88) وهو من المستوى المرتفع، حيث نصت الفقرة على (يشترط على الموظفين عدم إفشاء إجراءات الأمن والرقابة).

وفي المرتبة الأخيرة جاءت الفقرة رقم (9) بمتوسط حسابي (3.48) وبانحراف معياري (1.06)، وهو من المستوى المتوسط، حيث نصت الفقرة على (يتم متابعة المستخدمين وتسجيل الحوادث التي تخص أمن المعلومات داخل المكتبة).

جـ- واقع أمن البرمجية:

تم استخراج المتوسطات الحسابية والانحرافات المعيارية للتعرف إلى مستوى واقع أمن البرمجية بدوائر المعلومات في مكتبات الجامعات الأردنية، والجدول (8) يوضح ذلك:

الجدول (8)

المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة عن فقرات "واقع أمن البرمجية في مكتبات الجامعات الأردنية" مرتبة ترتيباً تنازلياً

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	الترتيب	المستوى
13	يتم التحقق من صحة البيانات المدخلة.	4.00	0.78	1	مرتفع
17	يتم حماية النظام عن طريق برامج مكافحة الفيروسات.	3.87	0.85	2	مرتفع
19	جميع برامج مكافحة الفيروسات والاختراق والتسلل موثوقة ومرخصة.	3.79	0.88	3	مرتفع
20	يتم تحديث برامج مكافحة الفيروسات والاختراق والتسلل بشكل مستمر.	3.61	1.05	4	متوسط
14	يتم استخدام آليات تشفير لحماية البيانات.	3.57	0.92	5	متوسط
16	تتوافر معايير لقبول أي نظم جديدة أو تعديل وإجراء اختبارات عليها قبل القبول بها.	3.52	0.98	6	متوسط
18	يتوفر برامج لتتبع الاختراق والتسلل.	3.38	1.00	7	متوسط
15	تتوافر تعليمات تضمن إجراء عملية التشفير بطريقة آمنة.	3.37	0.93	8	متوسط
	المتوسط العام الحسابي	3.63	0.78		مرتفع

يتضح من الجدول (8) أن المتوسطات الحسابية لـ (**واقع أمن البرمجية في مكتبات الجامعات الأردنية من وجهة نظر العاملين بدوائر المعلومات**)، تراوحت ما بين (3.37-4.00)، حيث حاز الواقع على متوسط حسابي إجمالي (3.63)، وهو من المستوى المتوسط، وقد حازت

الفقرة رقم (13) على أعلى متوسط حسابي حيث بلغ (4.00)، وبانحراف معياري (0.78)، وهو من المستوى المرتفع، وقد نصت الفقرة على (يتم التحقق من صحة البيانات المدخلة)، وفي المرتبة الثانية جاءت الفقرة رقم (17) بمتوسط حسابي بلغ (3.87) وبانحراف معياري (0.85) وهو من المستوى المرتفع، حيث نصت الفقرة على (يتم حماية النظام عن طريق برامج مكافحة الفيروسات).

وفي المرتبة الأخيرة جاءت الفقرة رقم (15) بمتوسط حسابي (3.37) وبانحراف معياري (0.93)، وهو من المستوى المرتفع، حيث نصت الفقرة على (تتوافر تعليمات تضمن إجراءات عملية التشفير بطريقة آمنة).

2- واقع سياسة أمن المعلومات

تم استخراج المتوسطات الحسابية والانحرافات المعيارية للتعرف إلى مستوى واقع سياسة أمن المعلومات بدوائر المعلومات في مكتبات الجامعات الأردنية، والجدول (9) يوضح ذلك:

الجدول (9)

المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة عن فقرات "واقع سياسة أمن المعلومات في مكتبات الجامعات الأردنية" مرتبة ترتيباً تنازلياً

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	الترتيب	المستوى
22	تحدد هذه السياسة المسؤوليات والصلاحيات مثل صلاحية منع المستخدم من الدخول للشبكة.	3.56	0.88	1	متوسط
21	يتوفر في المكتبة سياسة مكتوبة ومعتمدة لأمن المعلومات.	3.33	1.06	2	متوسط
23	تتضمن هذه السياسة إجراءات الوقاية من المخاطر.	3.29	0.90	3	متوسط
24	تتضمن هذه السياسة الإجراءات التي يجب اتباعها عند ظهور المشاكل.	3.27	0.96	4	متوسط
25	يتم مناقشة وتطوير سياسة أمن المعلومات بشكل دوري.	3.14	1.08	5	متوسط
	المتوسط العام الحسابي	3.32	0.82		متوسط

يتضح من الجدول (9) أن المتوسطات الحسابية لـ (**واقع سياسة أمن المعلومات في مكتبات الجامعات الأردنية من وجهة نظر العاملين بدوائر المعلومات**)، تراوحت ما بين (3.14-3.56)، حيث حاز الواقع على متوسط حسابي إجمالي (3.32)، وهو من المستوى المتوسط، وقد حازت الفقرة رقم (22) على أعلى متوسط حسابي حيث بلغ (3.56)، وبانحراف معياري (0.88)، وهو من المستوى المتوسط، وقد نصت الفقرة على (تحدد هذه السياسة المسؤوليات والصلاحيات مثل صلاحية منع المستخدم من الدخول للشبكة)، وفي المرتبة الثانية جاءت الفقرة رقم (21) بمتوسط حسابي بلغ (3.33) وبانحراف معياري (1.06) وهو من المستوى المتوسط، حيث نصت الفقرة على (يتوفر في المكتبة سياسة مكتوبة ومتعددة لأمن المعلومات).

وفي المرتبة الأخيرة جاءت الفقرة رقم (25) بمتوسط حسابي (3.14) وبانحراف معياري (1.08)، وهو من المستوى المتوسط، حيث نصت الفقرة على (يتم مناقشة وتطوير سياسة أمن المعلومات بشكل دوري).

3-واقع حماية البيانات الإلكترونية في المكتبة

تم استخراج المتوسطات الحسابية والانحرافات المعيارية للتعرف إلى مستوى واقع حماية البيانات الإلكترونية في مكتبات الجامعات الأردنية، والجدول (10) يوضح ذلك:

الجدول (10)

المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة عن فقرات "واقع حماية البيانات الإلكترونية في مكتبات الجامعات الأردنية" مرتبة ترتيباً تنازلياً

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	الترتيب	المستوى
26	يتوافر في المكتبة خدمة النسخ الاحتياطي لحماية البيانات الموجودة على الحاسوب.	3.65	1.09	1	متوسط
30	يتم تخزين وسائط البيانات الإلكترونية في أماكن خارجية آمنة.	3.61	0.99	2	متوسط
29	يتم تصنيف النسخ الاحتياطي حسب الفترة الزمنية التي تتم بها عملية النسخ لتسهيل الرجوع إليها.	3.55	1.02	3	متوسط
27	يتم متابعة عملية النسخ الاحتياطي للتأكد من أنها تتم بالشكل الصحيح.	3.51	1.06	4	متوسط
28	عندما تكون المعلومات المخزنة على وسائل النسخ الاحتياطي سرية يتم تشفيرها حسب السياسة المتبعة لذلك.	3.35	1.02	5	متوسط
31	يتم إتلاف وسائط التخزين الاحتياطي بطريقة آمنة عند إعادة استخدامها.	3.29	0.93	6	متوسط
	المتوسط العام الحسابي	3.49	0.85		متوسط

يتضح من الجدول (10) أن المتوسطات الحسابية لـ (**واقع حماية البيانات الإلكترونية في مكتبات الجامعات الأردنية من وجهة نظر العاملين بدوائر المعلومات**)، تراوحت ما بين (3.29-3.65)، حيث حاز الواقع على متوسط حسابي إجمالي (3.49)، وهو من المستوى المتوسط، وقد حازت الفقرة رقم (26) على أعلى متوسط حسابي حيث بلغ (3.65)، وبانحراف معياري (1.09)، وهو من المستوى المتوسط، وقد نصت الفقرة على (يتوافر في المكتبة خدمة النسخ الاحتياطي لحماية البيانات الموجودة على الحاسوب)، وفي المرتبة الثانية جاءت الفقرة رقم (30) بمتوسط حسابي بلغ (3.61) وبانحراف معياري (0.99) وهو من المستوى المتوسط، حيث نصت الفقرة على (يتم تخزين وسائط البيانات الإلكترونية في أماكن خارجية آمنة).

وفي المرتبة الأخيرة جاءت الفقرة رقم (31) بمتوسط حسابي (3.29) وبانحراف معياري (0.93)، وهو من المستوى المتوسط، حيث نصت الفقرة على (يتم إتلاف وسائط التخزين الاحتياطي بطريقة آمنة عند إعادة استخدامها).

4-واقع إجراءات حماية أنظمة وشبكات الحاسوب في المكتبة

تم استخراج المتوسطات الحسابية والانحرافات المعيارية للتعرف إلى مستوى واقع إجراءات حماية أنظمة وشبكات الحاسوب في مكتبات الجامعات الأردنية، والجدول (11) يوضح ذلك:

الجدول (11)

المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة عن فقرات "واقع إجراءات حماية أنظمة وشبكات الحاسوب في مكتبات الجامعات الأردنية" مرتبة ترتيباً تنازلياً

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	الترتيب	المستوى
33	يتم وضع كلمات مرور للدخول إلى الشبكة تعطى للأشخاص المخولين.	4.08	0.78	1	مرتفع
37	يتم أخذ الموافقة قبل التعديل على الأجهزة وبرامج الحماية.	3.87	0.85	2	مرتفع
34	يتوافر أجهزة تدعم حماية الشبكة الداخلية مثل أنظمة كشف ومنع الاختراق والجدران النارية fir wall وغيرها.	3.80	0.86	3	مرتفع
35	يتم ضبط الإعدادات الخاصة بالأجهزة الموجودة على الشبكات لتعمل بطريقة آمنة.	3.79	0.95	4	مرتفع
32	يتم تحديث نظم التشغيل في حال توجب ذلك (اختراق، خلل في عناصر الحماية الخاصة).	3.68	0.88	5	مرتفع
40	يتم تسجيل ما يحدث من أخطاء في نظم المعلومات في تقارير ويتم توثيق الإجراءات التي اتخذت لتصحيحها.	3.68	1.05	5	مرتفع
38	تحتفظ المكتبة بسجلات حول الأصول المكونة لكل نظام معلومات.	3.64	0.98	7	متوسط

39	في حال وجود إخفاق أو انقطاع في أداء الأعمال توجد خطة لإعادة الأعمال إلى طبيعتها ضمن إطار زمني مخطط.	3.61	0.97	8	متوسط
36	يتم رفع تقارير دورية توضح المشاكل الأمنية التي تمت مواجهتها على الشبكة.	3.45	0.86	9	متوسط
	المتوسط العام الحسابي	3.73	0.64		مرتفع

يتضح من الجدول (11) أن المتوسطات الحسابية لـ **(واقع إجراءات حماية أنظمة وشبكات الحاسوب في مكتبات الجامعات الأردنية من وجهة نظر العاملين بدوائر المعلومات)،** تراوحت ما بين (3.45-4.08)، حيث حاز الواقع على متوسط حسابي إجمالي (3.73)، وهو من المستوى المرتفع، وقد حازت الفقرة رقم (33) على أعلى متوسط حسابي حيث بلغ (4.08)، وبانحراف معياري (0.78)، وهو من المستوى المرتفع، وقد نصت الفقرة على (يتموضع كلمات مرور للدخول إلى الشبكة تعطى للأشخاص المخولين)، وفي المرتبة الثانية جاءت الفقرة رقم (37) بمتوسط حسابي بلغ (3.87) وبانحراف معياري (0.85) وهو من المستوى المرتفع، حيث نصت الفقرة على (يتم أخذ الموافقة قبل التعديل على الأجهزة وبرامج الحماية).

وفي المرتبة الأخيرة جاءت الفقرة رقم (36) بمتوسط حسابي (3.45) وبانحراف معياري (0.86)، وهو من المستوى المتوسط، حيث نصت الفقرة على (يتم رفع تقارير دورية توضح المشاكل الأمنية التي تمت مواجهتها على الشبكة).

5-واقع التحكم بالوصول لنظم المعلومات

تم استخراج المتوسطات الحسابية والانحرافات المعيارية للتعرف إلى مستوى واقع التحكم بالوصول لنظم المعلومات في مكتبات الجامعات الأردنية، والجدول (12) يوضح ذلك:

الجدول (12)

المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة عن فقرات "واقع التحكم بالوصول لنظم المعلومات في مكتبات الجامعات الأردنية" مرتبة ترتيباً تنازلياً

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	الترتيب	المستوى
41	يتم إعطاء مجموعة من الصلاحيات لكل مستخدم حسب المستوى الإداري.	4.04	0.95	1	مرتفع
46	هناك تقارير عن الأنشطة التي يقوم بها المستخدم.	3.76	0.99	2	مرتفع
42	يتم إعطاء كل مستخدم هوية خاصة به حيث لا يوجد صلاحيات عامة يستخدمها عدة أشخاص	3.75	0.98	3	مرتفع
45	يتم تسجيل العملية التي يقوم بها المستفيد بعد تنفيذها.	3.69	0.94	4	مرتفع
43	يتم إغلاق صلاحيات المستخدم لدواع متعلقة بأمن المعلومات.	3.62	1.05	5	متوسط
44	توجد مراجعات دورية لصلاحيات المستخدمين في الوصول للمعلومات.	3.61	0.97	6	متوسط
49	تستخدم سجلات الأداء لحفظ أنشطة المستخدم لدواع متعلقة بأمن المعلومات.	3.61	0.99	6	متوسط
48	بعض أنظمة المعلومات الحساسة معزولة في شبكات محلية مستقلة.	3.56	1.07	8	متوسط
47	تتوافر إرشادات لطريقة إنشاء كلمات مرور فورية.	3.46	1.12	9	متوسط
	المتوسط العام الحسابي	3.68	0.75		مرتفع

يتضح من الجدول (12) أن المتوسطات الحسابية لـ (**واقع إجراءات التحكم بالوصول لنظم المعلومات في مكتبات الجامعات الأردنية من وجهة نظر العاملين بدوائر المعلومات**)، تراوحت ما بين (3.46-4.04)، حيث حاز الواقع على متوسط حسابي إجمالي (3.68)، وهو من المستوى المرتفع، وقد حازت الفقرة رقم (41) على أعلى متوسط حسابي حيث بلغ (4.04)، وبانحراف معياري (0.95)، وهو من المستوى المرتفع، وقد نصت الفقرة على (يتم إعطاء مجموعة من الصلاحيات لكل مستخدم حسب المستوى الإداري)، وفي المرتبة الثانية جاءت الفقرة رقم (46) بمتوسط حسابي بلغ (3.76) وبانحراف معياري (0.99) وهو من المستوى المرتفع، حيث نصت الفقرة على (هناك تقارير عن الأنشطة التي يقوم بها المستخدم).

وفي المرتبة الأخيرة جاءت الفقرة رقم (47) بمتوسط حسابي (3.46) وبانحراف معياري (1.12)، وهو من المستوى المتوسط، حيث نصت الفقرة على (تتوافر إرشادات لطريقة إنشاء كلمات مرور فورية).

السؤال الثاني: ما الصعوبات التي تواجه العاملين في دوائر المعلومات في مكتبات الجامعات الأردنية؟

للإجابة عن السؤال الثاني، تم استخراج المتوسطات الحسابية والانحرافات المعيارية للتعرف إلى استجابات أفراد عينة الدراسة عن الصعوبات التي تواجه العاملين في دوائر المعلومات في مكتبات الجامعات الأردنية، والجدول (13) يوضح ذلك:

الجدول (13)

المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة عن فقرات "الصعوبات التي تواجه العاملين في دوائر المعلومات في مكتبات الجامعات الأردنية" مرتبة ترتيباً تنازلياً

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	الترتيب	المستوى
52	نقص الموظفين المتخصصين في أمن المعلومات	3.94	0.75	1	مرتفع
50	هناك نقص في الموازنة المخصصة لأمن المعلومات في المكتبة.	3.87	0.72	2	مرتفع
58	قلة الوقت الكافي لمناقشة الطرق الجديدة لحماية أمن المعلومات.	3.81	0.67	3	مرتفع
56	هناك صعوبات في تحديد حجم الخسارة الناجمة عن مختلف حوادث الانتهاك احيانا.	3.67	0.73	4	متوسط
60	ضعف التدريب على المهارات المطلوبة في مجال أمن المعلومات.	3.54	1.10	5	متوسط
57	يوجد صعوبات في تحديد كفاية الإجراءات الأمنية الحالية أو عدم كفايتها.	3.48	1.00	6	متوسط
59	ضعف الاهتمام من قبل الإدارة في الملاحظات التي رصدت.	3.48	1.15	6	متوسط
51	هناك صعوبة في توفير برامج لحماية أمن المعلومات الفعالة.	3.46	1.21	8	متوسط
53	هناك تزايد في إمكانية التعرض لمخاطر أمن المعلومات .	3.44	1.01	9	متوسط
54	صعوبة مواكبة الابتكارات والأساليب الحديثة في مجال أمن المعلومات.	3.43	1.01	10	متوسط
55	لا تتوافر الأدوات اللازمة التي تمكن المختصين بأمن المعلومات من تطوير عملهم.	3.42	1.09	11	متوسط
	المتوسط العام الحسابي	3.59	0.66		متوسط

يتضح من الجدول (13) أن المتوسطات الحسابية لـ (**الصعوبات التي تواجه العاملين في دوائر المعلومات في مكتبات الجامعات الأردنية**)، تراوحت ما بين (3.42-3.94)، حيث حازت الصعوبات على متوسط حسابي إجمالي (3.59)، وهو من المستوى المتوسط، وقد حازت الفقرة رقم (52) على أعلى متوسط حسابي حيث بلغ (3.94)، وبانحراف معياري (0.75)، وهو من المستوى المرتفع، وقد نصت الفقرة على (نقص الموظفين المتخصصين في أمن المعلومات)، وفي المرتبة الثانية جاءت الفقرة رقم (50) بمتوسط حسابي بلغ (3.87) وبانحراف معياري (0.72) وهو من المستوى المرتفع، حيث نصت الفقرة على (هناك نقص في الموازنة المخصصة لأمن المعلومات في المكتبة).

وفي المرتبة الأخيرة جاءت الفقرة رقم (55) بمتوسط حسابي (3.42) وبانحراف معياري (1.09)، وهو من المستوى المتوسط، حيث نصت الفقرة على (لا تتوافر الأدوات اللازمة التي تمكن المختصين بأمن المعلومات من تطوير عملهم).

السؤال الثالث: هل هناك فروق ذات دلالة إحصائية بين المتوسطات الحسابية لتقديرات العاملين بدوائر المعلومات في المكتبات الجامعية الأردنية لواقع أمن المعلومات تعزى إلى (الخبرة، ونوع الجامعة، والمستوى الوظيفي، والتخصص)؟

للإجابة عن السؤال الثالث، تم استخدام تحليل التباين Four Ways ANOVA، وذلك للتعرف إلى تقديرات العاملين بدوائر المعلومات في المكتبات الجامعية الأردنية لواقع أمن المعلومات تعزى إلى (الخبرة، ونوع الجامعة، والمستوى الوظيفي، والتخصص)، والجدول (14) يوضح ذلك:

الجدول (14):تحليل التباين (Four Ways ANOVA) للتعرف إلى الفروق في تقديرات العاملين بدوائر المعلومات في المكتبات الجامعية الأردنية لواقع أمن المعلومات تعزى إلى (الخبرة، ونوع الجامعة، والمستوى الوظيفي، والتخصص)

	المصدر	مجموع المربعات	df	متوسط المربعات	F	الدلالة الإحصائية
أمن البنية التحتية	Corrected Model	5.155[a]	7	.736	2.062	.058
	Intercept	289.122	1	289.122	809.457	.000
	الخبرة	.646	2	.323	.904	.409
	نوع_الجامعة	.131	1	.131	.368	.546
	المستوى_الوظيفي	1.016	2	.508	1.422	.248
	التخصص	2.519	2	1.260	3.527	*.034
	Error	27.146	76	.357		
	Total	1128.875	84			
	Corrected Total	32.301	83			
سياسة أمن المعلومات	Corrected Model	7.920a	7	1.131	1.815	.096
	Intercept	238.946	1	238.946	383.367	.000
	الخبرة	1.847	2	.923	1.481	.234
	نوع_الجامعة	1.197	1	1.197	1.920	.170
	المستوى_الوظيفي	.433	2	.217	.348	.708
	التخصص	2.991	2	1.496	2.400	.098
	Error	47.370	76	.623		
	Total	980.640	84			
	Corrected Total	55.290	83			
حماية البيانات الإلكترونية	Corrected Model	13.362a	7	1.909	3.145	.006
	Intercept	298.065	1	298.065	491.034	.000
	الخبرة	3.592	2	1.796	2.959	.058
	نوع_الجامعة	.037	1	.037	.061	.805
	المستوى_الوظيفي	4.442	2	2.221	3.659	*.030
	التخصص	3.244	2	1.622	2.672	.076
	Error	46.133	76	.607		
	Total	1083.833	84			
	Corrected Total	59.495	83			

إجراءات حماية أنظمة وشبكات الحاسوب في المكتبة	Corrected Model	7.771a	7	1.110	3.163	.005
	Intercept	318.697	1	318.697	907.959	.000
	الخبرة	1.190	2	.595	1.695	.190
	نوع_الجامعة	.014	1	.014	.040	.842
	المستوى_الوظيفي	1.599	2	.799	2.277	.110
	التخصص	4.234	2	2.117	6.032	*.004
	Error	26.676	76	.351		
	Total	1204.889	84			
	Corrected Total	34.447	83			
التحكم بالوصول لنظم المعلومات	Corrected Model	8.522a	7	1.217	2.440	.026
	Intercept	317.130	1	317.130	635.709	.000
	الخبرة	.958	2	.479	.961	.387
	نوع_الجامعة	.075	1	.075	.150	.699
	المستوى_الوظيفي	2.848	2	1.424	2.855	.064
	التخصص	3.591	2	1.796	3.599	*.032
	Error	37.913	76	.499		
	Total	1182.296	84			
	Corrected Total	46.435	83			

*دالة إحصائياً عند مستوى الدلالة (0.05)

أظهرت النتائج عدم وجود فروق ذات دلالة إحصائية تبعاً لمتغير (سنوات الخبرة)، حيث بلغت قيمة الإحصائي (F) (0.904، 1.481، 2.959، 1.695، 0.961) للمجالات بالترتيب وهي (أمن البنية التحتية، وسياسة أمن المعلومات، وحماية البيانات الإلكترونية، وإجراءات حماية أنظمة وشبكات الحاسوب في المكتبة، والتحكم بالوصول لنظم المعلومات) وجميع هذه القيم ليست دالة إحصائياً عند مستوى (α≤0.05).

وأظهرت النتائج عدم وجود فروق ذات دلالة إحصائية تبعاً لمتغير (نوع الجامعة)، حيث بلغت قيمة الإحصائي (F) (0.368، 1.920، 0.040،0.061، 0.150) للمجالات بالترتيب وهي (أمن البنية التحتية، وسياسة أمن المعلومات، وحماية البيانات الإلكترونية، وإجراءات حماية أنظمة وشبكات الحاسوب في المكتبة، والتحكم بالوصول لنظم المعلومات)، وجميع هذه القيم ليست دالة إحصائياً عند مستوى (α≤0.05).

وأظهرت النتائج وجود فروق ذات دلالة إحصائية تبعاً لمتغير (المستوى الوظيفي) في (حماية البيانات الإلكترونية)، حيث بلغت قيمة (F) (3.659)، وهذه القيمة دالة عند مستوى الدلالة الإحصائية (0.05≥α)، وأظهرت النتائج عدم وجود فروق ذات دلالة إحصائية تبعاً لمتغير (المستوى الوظيفي)، حيث بلغت قيمة الإحصائي (F) (1.422، 0.348، 2.277، 2.855) للمجالات بالترتيب وهي (أمن البنية التحتية، وسياسة أمن المعلومات، وإجراءات حماية أنظمة وشبكات الحاسوب في المكتبة، والتحكم بالوصول لنظم المعلومات)، وجميع هذه القيم ليست دالة إحصائياً عند مستوى (0.05≥α).

وتبين النتائج وجود فروق ذات دلالة إحصائية تبعاً لمتغير (التخصص) في (أمن البنية التحتية، وإجراءات حماية أنظمة وشبكات الحاسوب في المكتبة، والتحكم بالوصول لنظم المعلومات)، حيث بلغت قيمة (F) (3.527، 6.032، 3.599)، وهذه القيم دالة عند مستوى الدلالة الإحصائية (0.05≥α)، وأظهرت النتائج عدم وجود فروق ذات دلالة إحصائية تبعاً لمتغير (التخصص)، حيث بلغت قيمة الإحصائي (F) (2.400، 2.672) للمجالات بالترتيب وهي (سياسة أمن المعلومات، وحماية البيانات الإلكترونية)، وهذه القيم ليست دالة إحصائياً عند مستوى (0.05≥α).

وللتعرف إلى مصدر الفروق في حماية البيانات الالكترونية تبعاً للمستوى الوظيفي، ومصدر الفروق في أمن البنية التحتية، وإجراءات حماية أنظمة وشبكات الحاسوب في المكتبة، والتحكم بالوصول لنظم المعلومات تبعاً للتخصص، تم استخدام اختبار شيفيه، و نتائجهم مبينة فيما يلي:

جدول (15)

اختبار شيفيه للمقارنات البعدية للتعرف إلى الفروق في حماية البيانات الإلكترونية باختلاف المستوى الوظيفي

	(I) المستوى_الوظيفي	(J) المستوى_الوظيفي	الفرق بين المتوسطات	الدلالة الإحصائية
حماية البيانات الالكترونية	مدير	رئيس قسم	.84866	.230
		موظف	1.24466*	.040
	رئيس قسم	مدير	-.84866-	.230
		موظف	.39600	.114
	موظف	مدير	-1.24466*	.040
		رئيس قسم	-.39600-	.114

*دالة عند مستوى (0.05) فأقل

يتضح من الجدول (15) أن مصدر الفروق في حماية البيانات الإلكترونية كان لصالح فئة المديرين باختلاف المستوى الوظيفي لأفراد مجتمع الدراسة، أي أن هذه الفئة من أفراد مجتمع الدراسة ترى بأن البيانات محمية أكثر من رؤساء الأقسام والموظفين.

جدول (16)

اختبار شيفيه للمقارنات البعدية للتعرف إلى الفروق في أمن البنية التحتية، وإجراءات حماية أنظمة وشبكات الحاسوب في المكتبة، والتحكم بالوصول لنظم المعلومات باختلاف التخصص

	(I)التخصص	(J)التخصص	الفرق بين المتوسطات	الدلالة الاحصائية
أمن البنية التحتية	مكتبات ومعلومات	علم الحاسوب	-.28762-	.293
		تخصص آخر	.19936	.404
	علم الحاسوب	مكتبات ومعلومات	.28762	.293
		تخصص آخر	.48698*	.037
	تخصص آخر	مكتبات ومعلومات	-.19936-	.404
		علم الحاسوب	-.48698*	.037
إجراءات حماية أنظمة وشبكات الحاسوب في المكتبة	مكتبات ومعلومات	علم الحاسوب	-.48765*	.035
		تخصص آخر	.10262	.790
	علم الحاسوب	مكتبات ومعلومات	.48765*	.035
		تخصص آخر	.59028*	.010
	تخصص آخر	مكتبات ومعلومات	-.10262-	.790
		علم الحاسوب	-.59028*	.010
التحكم بالوصول لنظم المعلومات	مكتبات ومعلومات	علم الحاسوب	-.46065-	.040
		تخصص آخر	.03241	.856
	علم الحاسوب	مكتبات ومعلومات	.46065	.040
		تخصص آخر	.49306	.031
	تخصص آخر	مكتبات ومعلومات	-.03241-	.856
		علم الحاسوب	-.49306-	.031

*دالة إحصائياً عند مستوى الدلالة (0.05)

تظهر النتائج المبينة في الجدول (16) أن مصدر الفروق في أمن البنية التحتية، وإجراءات حماية أنظمة وشبكات الحاسوب في المكتبة، والتحكم بالوصول لنظم المعلومات، كان لصالح العاملين في مكتبات الجامعات الأردنية من فئة تخصص علم الحاسوب.

السؤال الرابع: هل هناك فروق بين المتوسطات الحسابية لتقديرات العاملين بدوائر المعلومات في المكتبات الجامعية الأردنية للصعوبات التي تواجه العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية تعزى إلى (الخبرة، ونوع الجامعة، والمستوى الوظيفي، والتخصص).

للإجابة عن السؤال الرابع، تم استخدام تحليل التباين (Four Ways ANOVA)، وذلك للتعرف إلى الصعوبات التي تواجه العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية تعزى إلى (الخبرة، ونوع الجامعة، والمستوى الوظيفي، والتخصص)، والجدول (17) يوضح ذلك:

الجدول (17)

تحليل التباين (Four Ways ANOVA) للتعرف إلى الصعوبات التي تواجه العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية تعزى إلى (الخبرة، ونوع الجامعة، والمستوى الوظيفي، والتخصص)

	المصدر	مجموعة المربعات	df	متوسط المربعات	F	الدلالة الاحصائية
الصعوبات	Corrected Model	3.676a	7	.525	1.230	.297
	Intercept	264.734	1	264.734	620.067	.000
	الخبرة	.081	2	.041	.095	.909
	نوع_الجامعة	.052	1	.052	.122	.728
	المستوى_الوظيفي	.485	2	.242	.568	.569
	التخصص	2.840	2	1.420	3.325	*.041
	Error	32.448	76	.427		
	Total	1120.579	84			
	Corrected Total	36.124	83			

*دالة إحصائياً عند مستوى الدلالة (0.05)

أظهرت النتائج وجود فروق ذات دلالة إحصائية تبعاً لمتغير (التخصص) في (الصعوبات التي تواجه العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية)، حيث بلغت قيمة (F) (3.325)، وهذه القيمة دالة عند مستوى الدلالة الإحصائية ($0.05\geq\alpha$)، وأظهرت النتائج عدم وجود فروق ذات دلالة إحصائية في الصعوبات التي تواجه العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية تبعاً لمتغير (الخبرة، ونوع الجامعة، والمستوى الوظيفي)، حيث بلغت قيمة

الإحصائي (F) (0.095، 0.122، 0.568)، وجميع هذه القيم ليست دالة إحصائياً عند مستوى (0.05≥α).

وللتعرف إلى مصدر الفروق في الصعوبات تبعاً للتخصص، تم استخدام اختبار شيفيه، والمبينة نتائجه في الجدول (18) الآتي:

جدول (18)

اختبار شيفيه للمقارنات البعدية للتعرف إلى الفروق في الصعوبات لدى العاملين في المكتبات في الجامعات الأردنية تبعا للتخصص

(I)التخصص	(J)التخصص	الفرق بين المتوسطات	الدلالة الاحصائية
مكتبات ومعلومات	علم الحاسوب	.42361*	.030
	تخصص آخر	-.10480-	.501
علم الحاسوب	مكتبات ومعلومات	-.42361*	.030
	تخصص آخر	-.52841*	.008
تخصص آخر	مكتبات ومعلومات	.10480	.501
	علم الحاسوب	.52841*	.008

يتضح من الجدول (18) أن مصدر الفروق في الصعوبات كان لصالح العاملين في مكتبات الجامعات الأردنية من فئة التخصصات الأخرى ومن ثم لصالح فئة تخصص المكتبات والمعلومات من أفراد مجتمع الدراسة.

الفصل الخامس

مناقشة النتائج والتوصيات

يتضمن هذا الفصل عرضا لمناقشة النتائج في ضوء أسئلة الدراسة التي هدفت إلى معرفة واقع أمن المعلومات من وجهة نظر العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية والصعوبات التي يواجهونها، كما يتضمن أيضا أهم التوصيات المقترحة في ضوء النتائج التي تم التوصل إليها والتي يؤمل أن تسهم في تحقيق أهداف هذه الدراسة.

أولاً: مناقشة النتائج:

مناقشة النتائج المتعلقة بالسؤال الأول : ما واقع أمن المعلومات من وجهة نظر العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية؟

للإجابة عن هذا السؤال، تم حساب المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد مجتمع الدراسة على الفقرات الخاصة بأمن المعلومات، وقد تم تقسيمها خمسة محاور هي: أمن البنية التحتية، وسياسة أمن المعلومات، وحماية البيانات الالكترونية، وحماية الأنظمة والشبكات، والتحكم بالوصول لنظم المعلومات. والجداول من (5- 12) توضح نتائج هذه المحاور.

أظهرت نتائج الجدول رقم (5) أن واقع أمن المعلومات من وجهة نظر العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية متوسط المستوى، إذ احتلت إجراءات أنظمة وشبكات الحاسوب في المكتبة المرتبة الأولى وبمستوى مرتفع، وتلاها التحكم بالوصول لنظم المعلومات بمستوى مرتفع، فيما جاء أمن البنية التحتية في المكتبات في المرتبة الثالثة وبمستوى متوسط، وجاءت حماية البيانات الإلكترونية وسياسة أمن المعلومات في المراتب الأخيرة على التوالي، وبمستوى متوسط.

وقد تعزى هذه النتيجة إلى أن أهم عامل في مكتبات الجامعات الأردنية هو إجراءات أنظمة وشبكات الحاسوب في المكتبة نظراً للاهتمام الكبير في هذا الأمر، وضرورة الالتزام بمتابعة أنظمة وشبكات الحاسوب لقضاء حاجة الطلبة من المكتبات. وكذلك الأمر فقد أظهرت الجامعات اهتماماً واضحاً في التحكم بالوصول لنظم المعلومات، من خلال البرامج والبوابات التي يستدل بها الطلاب على ما يلزمه من معلومات ومراجع، ومراجعة الأمور التي تلزم الطالب في المكتبة، وفيما يلي مناقشة فقرات الاستبانة لكل محور من محاور الدراسة:

1- واقع أمن البنية التحتية في المكتبات

- أظهرت نتائج الدراسة أن واقع البنية التحتية في المكتبات متوسط المستوى وذلك وفقاً لإجابات أفراد عينة الدراسة، حيث تمثل واقع أمن البنية التحتية من خلال الأبعاد الفرعية المتمثلة فيما يأتي:
- **واقع الأمن المادي في مكتبات الجامعات الأردنية:**

يتضح من الجدول (6) أن المتوسطات الحسابية لـواقع الأمن المادي في مكتبات الجامعات الأردنية من وجهة نظر العاملين بدوائر المعلومات، تراوحت ما بين (3.20-4.08)، حيث حاز الواقع على متوسط حسابي إجمالي (3.57)، وهو من المستوى المتوسط، وقد حازت (3) فقرات فقط على مستوى مرتفع بينما حازت باقي الفقرات على مستوى متوسط، ومن الجدير بالذكر أن الفقرات التي احتلت المراتب الثلاث الأولى هي على التوالي: الفقرة رقم (4) وهي "يتوافر أجهزة لكشف الحريق والإنذار حالة حدوثه"، وقد حازت على متوسط حسابي (4.08)، وبانحراف معياري (0.98)، وتفسر هذه النتيجة بأن المكتبات الجامعية تدرك أهمية هذا الأمر وخطورته البالغة على حياة الطلبة والعاملين ومصادر المعلومات والأجهزة ومرافق المكتبات، وإيمانا بأن الوقاية خير من العلاج حيث إن هذه الأجهزة تمكن فريق الطوارئ من التدخل الفوري فهي تسهم بشكل كبير في الحد من انتشار الحرائق، ويعزى أيضا إلى أن طبيعة المكتبات وبما تحتويه على مواد ورقية قابلة للاشتعال، يحتم على المكتبات الأخذ بالوسائل التي تحد من هذا الأمر. واتفقت هذه الدراسة بنسبة كبيرة مع دراسة با مفلح (2003) التي أشارت أن المكتبة مؤمنة من الناحية المادية وذلك بتطبيق إجراءات خاصة بالمكان مثل أجهزة الإنذار وكشف الحريق وغيرها.

وحصلت الفقرة رقم (8) وهي" يمنع الموظف غير المختص من إجراء أي تعديل مادي على الأجهزة في المكتبة"، على متوسط حسابي (3.93)، وبانحراف معياري (0.98)، ويعزى ذلك لأهمية المعلومات التي تحتويها هذه الأجهزة، فلا يمكن أي شخص غير موظف أو مختص بالصيانة إجراء أي تعديل على الأجهزة، بالإضافة أو التعديل أو الحذف لأي برنامج أو أي إجراء يمكن أن يؤثر على أداء الأجهزة، واتفقت هذه النتيجة مع دراسة الدنف (2013) التي أشارة أنه يمنع الموظف غير المختص من إجراء تعديلات أمنية على الأجهزة ضمن نظم المعلومات، فيما أشارت اسماعيل (2012) إلى أن هناك أخطاء تحدث أثناء صيانة الأجهزة. وحصلت الفقرة رقم (2) وهي " جميع كوابل الكهرباء والاتصالات التي تنقل البيانات محمية من العبث بها أو الإتلاف داخل

المكتبة"، وقد حصلت على متوسط حسابي (3.68)، وبانحراف معياري (1.16). وهي نتيجه مهمة فهذا يزيد من مستوى الأمن في المكتبات والتقليل من المخاطر المحتملة مما يزيد الثقة لدى الطلبة بالمكتبة ويشعرهم بالأمان نتيجة المحافظة على الكبلات الكهربائية وكبلات الاتصالات، ويزيد من مستوى مراجعتهم للمكتبات. وتتفق هذه النتيجة مع دراسة السريحي (2002) ودراسة با مفلح (2003) التان أشارتا إلى أن المكتبات تتخذ إجراءات عديدة لتأمين التمديدات الكهربائية وخطوط الاتصالات.

وفي المرتبة الأخيرة جاءت الفقرة رقم (1) بمتوسط حسابي (3.20) وبانحراف معياري (1.42)، وهو من المستوى المتوسط، حيث نصت الفقرة على "يوجد مصدر احتياطي للكهرباء داخل المكتبة)، يعزى ذلك إلى أن المصادر البديلة متوفرة أساسا في كثير من الجامعات التي تتبع لها هذه المكتبات حيث إن الجامعات الأردنية توفر مصدرا بديلا للطاقة لكافة مرافقها في حال إنقطاع الكهرباء، وقد تعزى ايضا إلى قلة إهتمام إدارة المكتبات بأهمية توافر مصدر بديل للطاقة خاص بالمكتبة نظرا لخصوصية المكتبة التي في كثير من الأحيان تكون ساعات العمل بها تمتد لأوقات متأخرة، وما تحتويه من مصادر أيضا، يجعل تأثرها بانقطاع الطاقة أكبر من مرافق الجامعة الأخرى. واتفقت هذه النتيجة مع دراسة با مفلح (2003) التي أشارت إلى عدم توافر أجهزة في المكتبات توفر الطاقة في حال اقطاعها.

- **واقع حماية الأفراد في مكتبات الجامعات الأردنية:**

يتضح من الجدول (7) أن المتوسطات الحسابية لواقع حماية الأفراد في مكتبات الجامعات الأردنية من وجهة نظر العاملين بدوائر المعلومات، تراوحت ما بين (3.48-3.83)، حيث حاز الواقع على متوسط حسابي إجمالي (3.63)، وهو من المستوى المتوسط، وقد حازت الفقرة رقم (12) على أعلى متوسط حسابي حيث بلغ (3.83)، وبانحراف معياري (0.94)، وهو من المستوى المرتفع، وقد نصت الفقرة على "يتم محاسبة الموظف الذي ينتهك إجراءات أمن المعلومات داخل المكتبة"، وقد تعزى هذه النتيجة إلى الإجراءات الصارمة التي تتمتع بها الجامعات وخصوصاً المكتبات، لتشكل رادعا لكل موظف يحاول أن ينتهك إجراءات الأمن في المكتبة، مما يحافظ على أمن أنظمة المكتبة ومصادرها وخصوصية وسرية العاملين والطلبة، فلدقة المعلومات ومصداقيتها الأثر البالغ في ثقة الطلبة لمراجعة المكتبات، وعندما يحصل أي تغيير أو تعديل أو تزييف للمعلومات، فهذا حتماً سوف يؤثر على أمن المعلومات في المكتبات.

وفي المرتبة الثانية جاءت الفقرة رقم (11) بمتوسط حسابي بلغ (3.69) وبانحراف معياري (0.88) وهو من المستوى المرتفع، حيث نصت الفقرة على أنه "يشترط على الموظفين عدم إفشاء إجراءات الأمن والرقابة". ويعزى ذلك لحرص المكتبات الجامعية على التزام موظفيها بالمعايير والقواعد الأخلاقية لعدم إفضاء الموظفين بمعلومات لها صفة السرية وذلك للحفاظ على الأمن والسرية بالشكل الصحيح فعندما يفصح أو يفشي الموظفون عن إجراءات الأمن والرقابة يصبح من السهل لأي شخص أكان موظفاً أو غير موظف أن يخترق الشبكات أو يخترق الأماكن أو يعبث بالأجهزة وتغيير ما يشاء وتعطيل الأجهزة ونشر ما يرغب على المواقع الخاصة بالمكتبات دون أن يشعر به أحد، فلهذا الأمر الأهمية البالغة من وجهة نظر أفراد عينة الدراسة.

وفي المرتبة الأخيرة جاءت الفقرة رقم (9) بمتوسط حسابي (3.63) وبانحراف معياري (1.06) وهو من المستوى المتوسط، وقد نصت على "يتم متابعة المستخدمين وتسجيل الحوادث التي تخص أمن المعلومات" . وقد تفسر هذه النتيجة بقلة الوعي لدى إدارة المكتبات والعاملين بدوائر المعلومات بأهمية توثيق الحوادث التي تخص أمن المعلومات للاستفادة من الأخطاء التي تحدث ومحاولة تلافيها وعدم تكرارها.

- **واقع أمن البرمجية في مكتبات الجامعات الأردنية:**

يتضح من الجدول (8) أن المتوسطات الحسابية لواقع أمن البرمجية في مكتبات الجامعات الأردنية من وجهة نظر العاملين بدوائر المعلومات، تراوحت ما بين (3.37-4.00)، حيث حاز الواقع على متوسط حسابي إجمالي (4.00)، وهو من المستوى المرتفع، وقد حازت الفقرة رقم (13) على أعلى متوسط حسابي حيث بلغ (4.00)، وبانحراف معياري (0.78)، وهو من المستوى المرتفع، وقد نصت الفقرة على "يتم التحقق من صحة البيانات المدخلة"، ويعزى ذلك إلى أن المكتبات بطبيعتها تحتاج لمراجعة وتدقيق البيانات أكثر من مرة في كثير من الأحيان مثل البيانات الببلوغرافية لمصادر المعلومات وقواعد البيانات وغيرها، وهذا الأمر بالغ الأهمية والحساسية ويعتبر أساسا للبيانات أو المعلومات أو المراجع التي يستنير بها الطلبة وعمل الأبحاث والدراسات عليها، فلا بد أن تكون هذه البيانات صحيحة وبدرجة عالية المستوى لأنها أساس محتوى المكتبات فعلياً، وفي المرتبة الثانية جاءت الفقرة رقم (17) بمتوسط حسابي بلغ (3.87) وبانحراف معياري (0.85) وهو من المستوى المرتفع، حيث نصت الفقرة على "يتم حماية النظام عن طريق برامج مكافحة الفيروسات". ويعزى ذلك إلى أهمية لحفاظ على أمن البرمجيات ودوام استمرارية التعامل مع البرامج والمواقع دون حدوث أي خلل أو أي اختراق لتلك المواقع، وتعتبر هذه البرامج في غاية الأهمية في رفع مستوى أمن المعلومات في المكتبات. واتفقت هذه الدراسة مع غالبية الدراسات السابقة، مثل دراسة العربي (2012)، والدنف

(2013)، وعمار (2011)، والزهيمي (2010)، والهادي (2006)، وبا مفلح (2003)، ومايدبينو وأوانج (Maidabino &Awang (2011، وإسماعيل (Ismail (2012، حيث أشارت هذه الدراسات إلى أن المكتبات والمؤسسات تهتم بوجود برامج الحماية من الفيروسات لما لهذا الأمر من أهمية.

وحصلت الفقرة رقم (19) على مستوى مرتفع بمتوسط حسابي (3,79)، وانحراف معياري (0,88) وتنص على "جميع برامج مكافحة الفيروسات والاختراق والتسلل موثوقة ومرخصة" ويمكن أن يعزى ذلك إلى تزايد ظهور نسخ مزورة من هذه البرامج، فقد ظهرت في بعض البلدان نسخ مقرصنة من هذه البرامج، ما يؤدي إلى نتيجة عكسية و حرص المكتبات الجامعية على توفير برامج موثوقة لمكافحة الفيروسات والتسلل والاختراق للحفاظ على أجهزة وبرامج وشبكات المكتبات من المواد الضارة.

وفي المرتبة الأخيرة جاءت الفقرة رقم (15) بمتوسط حسابي (3.37) وبانحراف معياري (0.93)، وهو من المستوى المتوسط، حيث نصت الفقرة على "تتوافر تعليمات تضمن إجراءات عملية التشفير بطريقة آمنة". وهي نتيجة غير متوقعة، ومن الممكن أن تعزى هذه النتيجة إلى قلة اعتماد المكتبات الجامعية أساسا على تشفير البيانات. وقد تعزى أيضا إلى قلة الوعي في وجود تعليمات تحقق عملية تشفير بشكل مناسب، فالتشفير قد لا يكون فعالا إذا لم يستخدم بالشكل المناسب، ففي ظل عدم وجود تعليمات من الممكن أن يكون التشفير ضعيفا بل يعتبر أسوأ من عدم التشفير، فقد يعطي إحساسا كاذبا بالأمن. اتفقت هذه النتيجة مع دراسة با مفلح (2003) التي أشارت قلة الاهتمام ببعض الأساليب الأمنية الضرورية ومن أهمها نظام التشفير.

2- واقع سياسة أمن المعلومات في مكتبات الجامعات الأردنية:

يتضح من الجدول رقم (9) أن المتوسطات الحسابية لواقع سياسة أمن المعلومات في مكتبات الجامعات الأردنية من وجهة نظر العاملين بدوائر المعلومات تراوحت ما بين (3.14-3.56)، حيث حاز الواقع على متوسط حسابي إجمالي (3.32)، وهو من المستوى المتوسط، وقد حازت الفقرة رقم (22) على أعلى متوسط حسابي حيث بلغ (3.56)، وبانحراف معياري (0.88)، وهو من المستوى المتوسط، وقد نصت الفقرة على "تحدد هذه السياسة المسؤوليات والصلاحيات مثل صلاحية منع المستخدم من الدخول للشبكة"، وقد تعزى هذه النتيجة إلى أن معظم العاملين أو المستخدمين للشبكات داخل المكتبات يحتفظون برقم سري أو بكلمات سرية لا يمكن حذفها أو تعديلها بالشكل المطلق عند تحديد مشكلة ما إلا بإجراءات قد تأخذ من المسؤولين

الوقت وإبلاغ صاحب الحساب بأنه ممنوع من استخدام الخدمة أو الدخول إلى الشبكة وهذا قد يعيق العمل داخل المكتبة ويسبب بعض الإرباكات التي قد تسببها في بعض الأحيان.

وفي المرتبة الثانية جاءت الفقرة رقم (21) بمتوسط حسابي بلغ (3.33) وبانحراف معياري (1.06) وهو من المستوى المتوسط، حيث نصت الفقرة على "يتوفر في المكتبة سياسة مكتوبة ومتعددة لأمن المعلومات"، وتعزى هذه النتيجة إلى أن إدارات المكتبات الجامعية لا تدرك أهمية سياسة أمن المعلومات ونقص الوعي الأمني المترتب على عدم الاهتمام بهذه السياسة التي تعتبر إحدى أهم الوسائل للمحافظة على أمن المعلومات في المكتبات التي لا تتوقف على منع الجريمة فحسب، بل تشمل المحافظة على وقت العاملين وعدم استخدامهم لما ليس له علاقة بالعمل كالإنترنت وغيرها، وتحديد أطر إجراءات العمل والأدوار والمسؤوليات والواجبات العامة. وتتفق هذه النتيجة مع دراسة السريحي (2002)، و دراسة مايدبينو وأوانج (2011) Maidabino and Awang ، ودراسة إسماعيل وأوانج (2011) Ismail and Awang، ودراسة السريحي (2002)، ودراسة الهادي (2006)، ودراسة عمار (2011)، ودراسة الزهيمي (2010)، ودراسة العربي (2012)، ودراسة الدنف (2013)، حيث أشارت هذه الدراسات إلى قلة اهتمام المكتبات والمؤسسات التعليمية بوجود سياسة واضحة ومكتوبة لأمن المعلومات.

وفي المرتبة الأخيرة جاءت الفقرة رقم (25) بمتوسط حسابي (3.14) وبانحراف معياري (1.08)، وهو من المستوى المتوسط، حيث نصت الفقرة على "يتم مناقشة وتطوير سياسة أمن المعلومات بشكل دوري". ويعزى ذلك لعدم الاهتمام بالسياسة الأمنية، ويؤكد النتيجة السابقة، وهي قلة الاهتمام بوجود سياسة واضحة ومكتوبة لأمن المعلومات تتبعها المكتبات الجامعية وهذا يعيق الإدارة في تحقيق مستوى عال من الأمن ويعيق كذلك المحافظة على أمن المعلومات في المكتبات الجامعية.

3- واقع حماية البيانات الإلكترونية بدوائر المعلومات في مكتبات الجامعات الأردنية:

يتضح من الجدول (10) أن المتوسطات الحسابية لواقع حماية البيانات الإلكترونية في مكتبات الجامعات الأردنية من وجهة نظر العاملين بدوائر المعلومات، تراوحت ما بين (3.29-3.65)، حيث حاز الواقع على متوسط حسابي إجمالي (3.49)، وهو من المستوى المتوسط، وقد حازت الفقرة رقم (26) على أعلى متوسط حسابي حيث بلغ (3.65)، وبانحراف معياري (1.09)، وهو من المستوى المتوسط، وقد نصت الفقرة على "يتوافر في المكتبة خدمة النسخ الاحتياطي لحماية البيانات الموجودة على الحاسوب"، وقد تعزى هذه النتيجة إلى أن دوائر المعلومات في المكتبات ليس لديها الوعي الكافي بأن هناك حاجة ماسة لحماية البيانات الموجودة

على الحاسوب، فربما عند استخدام أحد الطلبة لجهاز الحاسوب يتم تعطيله لأي سبب من الأسباب أو خطأ في الاستخدام أو لخلل ميكانيكي داخل الجهاز أو عطل كهربائي، وبهذا يتم حذف واختفاء المعلومات المنسوخة على هذا الجهاز، فلا بد أن تعمل دوائر المعلومات على الاهتمام بخدمة النسخ الاحتياطي تقوم بحفظ المعلومات على وسائط مخصصة لذلك يتم من خلالها استرجاع ما يرغب الموظف باسترجاعه عند الضرورة دون أي عوائق تذكر، وتتفق هذه النتيجة إلى حد ما دراسة العربي (2012) التي أشارت إلى ضعف امتلاك المؤسسات التعليمية لنسخ احتياطية من البيانات، ودراسة الزهيمي (2010) التي أشارت لعدم وجود بعض الاجراءات الأمنية مثل خدمة النسخ الاحتياطي.

وفي المرتبة الثانية جاءت الفقرة رقم (30) بمتوسط حسابي بلغ (3.61) وبانحراف معياري (0.99) وهو من المستوى المتوسط، حيث نصت الفقرة على "يتم تخزين وسائط البيانات الالكترونية في أماكن خارجية آمنة"، ويعزى ذلك إلى قلة الوعي بضرورة الحفاظ على هذه النسخ بطريقة آمنة لاسترجاعها في حالات قد تتعرض فيها المكتبة للمخاطر، وإذا لم يتم ذلك فأن جميع البيانات المخزنة على هذه الوسائط تكون مهددة بالتلف أوالمخاطر المختلفة، فهذه الوسائط تخزن عليها بيانات مهمة ويجب أن تحظى بالاهتمام.

وفي المرتبة الأخيرة جاءت الفقرة رقم (31) بمتوسط حسابي (3.29) وبانحراف معياري (0.93)، وهو من المستوى المتوسط، حيث نصت الفقرة على "يتم إتلاف وسائط التخزين الاحتياطي بطريقة آمنة عند إعادة استخدامها"، وتعزى هذه النتيجة إلى الأسلوب التقليدي في إتلاف هذه الوسائط، وهذا قد يعرضها لكشف محتويات هذه الوسائط من الأشخاص الذين يجدونها.

4- واقع إجراءات حماية أنظمة وشبكات الحاسوب في مكتبات الجامعات الأردنية:

يتضح من الجدول (11) أن المتوسطات الحسابية لواقع إجراءات حماية أنظمة وشبكات الحاسوب في مكتبات الجامعات الأردنية من وجهة نظر العاملين بدوائر المعلومات، تراوحت ما بين (3.45-4.08)، حيث حاز الواقع على متوسط حسابي إجمالي (3.73)، وهو من المستوى المرتفع، وقد حازت الفقرة رقم (33) على أعلى متوسط حسابي حيث بلغ (4.08)، وبانحراف معياري (0.78)، وهو من المستوى المرتفع، وقد نصت الفقرة على "يتم وضع كلمات مرور للدخول إلى الشبكة تعطى للأشخاص المخولين"، وقد تعزى هذه النتيجة إلى أن معظم مكتبات الجامعات الأردنية تعمل على المحافظة على هذا الأمر، وذلك حفاظاً وحماية لأنظمة وشبكات الحاسوب، فبكلمات المرور تضمن إدارة مكتبات الجامعات الأردنية عدم التسلل إلى المواقع

الخاصة بالمكتبات أو بالمواقع الخاصة بالرسائل الجامعية وغيرها. وفي المرتبة الثانية جاءت الفقرة رقم (37) بمتوسط حسابي بلغ (3.87) وبانحراف معياري (0.85) وهو من المستوى المرتفع، حيث نصت الفقرة على "يتم أخذ الموافقة قبل التعديل على الأجهزة وبرامج الحماية". وذلك نظراً لأهمية الموضوع من الناحية الإجرائية والتطبيقية، فعند التعديل على الأجهزة وبرامج الحماية تصبح لدى العاملين الفكرة التامة بطريقة التشغيل الحديثة أو استخدام البرامج والمواقع، فهذا كله يعود بالفائدة على حماية الأنظمة والشبكات في مكتبات الجامعات الأردنية.

وحصلت الفقرة (34) على متوسط حسابي (3.80) وانحراف معياري (0.86) وهو من المستوى المرتفع، وتنص "يتوافر أجهزة تدعم حماية الشبكة الداخلية مثل أنظمة كشف ومنع الاختراق والجدران النارية وغيرها"، ويعزى ذلك إلى أن المكتبات الجامعية تحرص على حماية أنظمتها وشبكاتها من الوصول غير المرغوب به أو تعطيلها والتلاعب بها من خلال الاختراقات التي قد تحصل أو استخدام برامج ضارة أو أية تصرفات يمكن أن تنتهك أنظمة المكتبات وشبكاتها. اتفقت في ذلك مع دراسة عمار (2011) التي أشارت إلى أن المؤسسات التي تعتمد على تقنية المعلومات في تسيير أعمالها وتوفر أجهزة لحماية شبكاتها مثل وسيط (Proxy) وجدران حماية، وتختلف في ذلك مع دراسة با مفلح (2003) التي أشارت إلى أن المكتبة تفتقد لبعض أساليب الحماية الضرورية مثل الجدران النارية.

وفي المرتبة الأخيرة جاءت الفقرة رقم (36) بمتوسط حسابي (3.45) وبانحراف معياري (0.86)، وهو من المستوى المتوسط، حيث نصت الفقرة على "يتم رفع تقارير دورية توضح المشاكل الأمنية التي تمت مواجهتها على الشبكة"، وهي نتيجة غير متوقعة حيث لا بد من رفع هذه التقارير وذلك لمعالجة الأخطاء أو أية مشكلة يمكن أن تحدث في أنظمة وشبكات المكتبة فكلمات المرور وبرامج الحماية غير كافية ومن الممكن أن تظهر فيها مشكلات أثناء تطبيقها، فيجب أن تتعرف المكتبات على هذه المشاكل عن طريق التقارير الدورية حتى يتسنى التعديل والضبط لهذه الأنظمة.

5- واقع التحكم بالوصول لنظم المعلومات في مكتبات الجامعات الأردنية:

يتضح من الجدول (12) أن المتوسطات الحسابية لواقع إجراءات التحكم بالوصول لنظم المعلومات في مكتبات الجامعات الأردنية من وجهة نظر العاملين فيها، تراوحت ما بين (3.46-4.04)، وبمتوسط حسابي كلي (3.68)، وانحراف معياري (0.75)، وبدرجة كلية متوسطة، وقد حازت الفقرة رقم (41) على أعلى متوسط حسابي حيث بلغ (4.04)، وبانحراف معياري

(0.95)، وهو من المستوى المرتفع، وقد نصت الفقرة على (يتم إعطاء مجموعة من الصلاحيات لكل مستخدم حسب المستوى الإداري)، وقد تعزى هذه النتيجة إلى إعطاء مجموعة من الصلاحيات لكل مستخدم وذلك للتصرف بما يراه مناسباً عند حدوث مشكلة وحلها بالشكل المناسب في نظم المعلومات، وهذه الصلاحيات للمجموعات تحتاج إلى بطاقات خاصة تثبت هذه البطاقات أن لهم الصلاحيات في معالجة الأخطاء أو تغيير بعض البيانات ونقلها من مكان إلى مكان داخل الموقع بالإضافة إلى نشر بعض المقالات أو المعلومات الحديثة على المواقع الخاصة بالجامعات من خلال المكتبات، وذلك لرفع مستوى واقع التحكم بالوصول لنظم المعلومات، وتتفق هذه النتيجة مع دراسة بامفلح (2003) التي أشارت إلى عدم تحديد صلاحيات المستستخدمين من الموظفين وفقا لعملهم الفعلي بالمكتبة، ودراسة السريحي (2002)، وفي المرتبة الثانية جاءت الفقرة رقم (46) بمتوسط حسابي بلغ (3.76) وبانحراف معياري (0.99) وهو من المستوى المرتفع، حيث نصت الفقرة على "هناك تقارير عن الأنشطة التي يقوم بها المستخدم". وتؤكد هذه النتيجة حرص المكتبات على متابعة صلاحيات الدخول ومعالجة الأخطاء التي قد تظهر .

وفي المرتبة الأخيرة جاءت الفقرة رقم (47) بمتوسط حسابي (3.46) وبانحراف معياري (1.12)، وهو من المستوى المتوسط، حيث نصت الفقرة على (تتوافر إرشادات لطريقة إنشاء كلمات مرور قوية) ويعزى ذلك إلى عدم الاهتمام والوعي من قبل إدارة المكتبات ودوائر المعلومات بالمحافظة على خصوصية العاملين بالمكتبات وخصوصا المشرفين على الأنظمة وبما توفره هذه الإرشادات من وقت وجهد للمستخدمين . واختلفت نتيجة هذه الدراسة مع دراسة الدنف (2013) التي أكدت وجود إرشادات لإنشاء كلمات المرور القوية.

مناقشة النتائج المتعلقة بالسؤال الثاني: ما الصعوبات التي تواجه العاملين في دوائر المعلومات في التصدي للانتهاكات الإلكترونية في مكتبات الجامعات الأردنية ؟

يظهر من الجدول رقم (13) المتوسطات الحسابية، والانحرافات المعيارية، والدرجة الكلية لموافقة العاملين بدوائر المعلومات على الصعوبات التي تواجههم بمتوسط حسابي كلي (3.59) وبانحراف معياري (0.66)، وهذا يدل على أن العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية يواجهون صعوبات في عملهم بشكل عام وفي مجال أمن المعلومات بشكل خاص، ما يدل على أن المكتبات الجامعية لا تواكب التطور الذي يطرأ على مجال أمن المعلومات بالشكل المطلوب ولا تحقق التطلعات المنشودة في هذا المجال.

وفيما يلي عرض تحليلي لأهم الصعوبات التي تواجه العاملين حسب تقديرهم، فقد احتلت الفقرة رقم (52) المرتبة الأولى وبمستوى مرتفع، وبمتوسط حسابي (3.94)، وبانحراف معياري (0.75)، وتنص "نقص الموظفين المتخصصين في أمن المعلومات"، وقد تعزى هذه النتيجة إلى أن الجامعات الأردنية ترى أن عدد الموظفين كاف في ظل الموازنات المرصودة حالياً للرواتب الخاصة بالموظفين، وقد تعزى أيضا إلى قلة الوعي بوجوب وجود موظفين متخصصين وأكفياء في مجال أمن المعلومات أو التخصصات التقنية ذات العلاقة وذلك لرفع مستوى الأمن والحماية في هذه المكتبات. واتفقت هذه النتيجة في ذلك مع دراسة مايدبينو وأوانج (2011) Maidabino & Awang، ودراسة السريحي (2002) اللتان أشارتا إلى عدم وجود فريق مختص في يشرف على النظم الآلية في المكتبة على الرغم من أهمية هذا الأمر لتحقيق الأمن، ودراسة عمار (2011)، التي أشارت إلى قلة الخبرة بأمن المعلومات لدى العاملين في المؤسسات التعليمية.

وحصلت الفقرة رقم (50) على متوسط حسابي (3.87)، بانحراف معياري (0.72) بمستوى مرتفع، وقد نصت على " هناك نقص في الموازنة المخصصة لأمن المعلومات في المكتبة"، وحصلت الفقرة رقم (58) على متوسط حسابي (3.81)، وبانحراف معياري (0.67) بمستوى عال، وقد نصت على " قلة الوقت الكافي لمناقشة الطرق الجديدة لحماية أمن المعلومات" وتؤكد هاتان الفقرتان ما جاء في الفقرة السابقة حيث يرى الباحث أن دوائر المعلومات في مكتبات الجامعات الأردنية ليس لديها الوقت الكافي لمناقشة الطرق الجديدة لحماية أمن المعلومات، وذلك لأن معظم العاملين ليس لديهم أية ترتيبات لعقد الاجتماعات بعد انقضاء أوقات دوامهم أو خلالها، وهذا متعلق بعدد الموظفين، فكلما زاد عدد الموظفين توفر الوقت الكافي لبعض الموظفين الآخرين لعقد الاجتماعات لمناقشة الطرق الجديدة لحماية أمن المعلومات والموظفين الآخرين الذين يعملون فبهذا يتم التنسيق وتتضح النتائج، وبالتالي سيؤدي إلى صعوبة في حصر حجم الخسارة الناتجة عن مختلف حوادث الانتهاك وتقييم الوضع الأمني بشكل عام. وتتفق في ذلك مع دراسة اللوزي (2003) التي أشارت إلى أن الموارد المادية من أهم الصعوبات التي تواجه أمن المعلومات.

مناقشة النتائج المتعلقة بالسؤال الثالث: هل هناك فروق ذات دلالة إحصائية بين المتوسطات الحسابية لتقديرات العاملين بدوائر المعلومات في المكتبات الجامعية الأردنية لواقع أمن المعلومات تعزى إلى (الخبرة، ونوع الجامعة، والمستوى الوظيفي، والتخصص)؟

بين الجدول رقم (14) المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد مجتمع الدراسة حول واقع أمن المعلومات وفقا لمتغيرات (الخبرة، ونوع الجامعة، والمستوى

الوظيفي، والتخصص)، وقد تم إجراء تحليل التباين الرباعي وأظهرت النتائج عدم وجود فروق ذات دلالة إحصائية تبعاً لمتغير سنوات الخبرة، ونوع الجامعة. وقد تعزى هذه النتيجة إلى أن العاملين سواء كانوا من ذوي خبرة كبيرة أو قليلة في الجامعات الحكومية أو الخاصة، لديهم نفس التقدير لواقع أمن المعلومات نظرا للتشابه في الأدوار في المكتبات الجامعية والخاصة وحداثة خبرات هذه الفئة وحاجتها لاثبات قدراتها وتعزيز مهاراتها.

وأظهرت النتائج وجود فروق ذات دلالة إحصائية تبعاً لمتغير (المستوى الوظيفي) في (حماية البيانات الإلكترونية)، وتبين أن مصدر الفروق في حماية البيانات الإلكترونية كان لصالح فئة المديرين باختلاف المستوى الوظيفي لأفراد مجتمع الدراسة، أي أن هذه الفئة من أفراد مجتمع الدراسة ترى أن البيانات محمية أكثر من رؤساء الاقسام والموظفين. وربما يعزى ذلك لطبيعة عمل فئة المديرين فهم يقومون بالإشراف والتوجيه، ولكن قد يختلف التطبيق عن التوجيه مما جعل هذه الفئة تختلف مع الفئات الأخرى في هذا المحور.

وتبين النتائج وجود فروق ذات دلالة إحصائية تبعاً لمتغير (التخصص) في (أمن البنية التحتية، وإجراءات حماية أنظمة وشبكات الحاسوب في المكتبة، والتحكم بالوصول لنظم المعلومات). وتبين أن مصدر الفروق في أمن البنية التحتية، وإجراءات حماية أنظمة وشبكات الحاسوب في المكتبة، والتحكم بالوصول لنظم المعلومات، كان لصالح العاملين في مكتبات الجامعات الأردنية من فئة تخصص علم الحاسوب، وقد يعزى ذلك لمعرفتهم بالأمور التقنية أكثر تخصص علم المكتبات والمعلومات والتخصصات الأخرى؛ فعلم الحاسوب أقرب للتخصصات التقنية وهذا ما يجعله يختلف في وجهة نظرهم في بعض محاور الدراسة.

مناقشة النتائج المتعلقة بالسؤال الرابع: هل هناك فروق بين المتوسطات الحسابية لتقديرات العاملين بدوائر المعلومات في المكتبات الجامعية الأردنية للصعوبات التي تواجه العاملين بدوائر المعلومات في التصدي للانتهاكات الإلكترونية في مكتبات الجامعات الأردنية تعزى إلى (الخبرة، ونوع الجامعة، والمستوى الوظيفي، والتخصص)؟

تظهر النتائج في الجدول رقم (17) المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد مجتمع الدراسة حول تقديراتهم للصعوبات التي تواجههم وفقا لمتغيرات الدراسة (الخبرة، ونوع الجامعة، والمستوى الوظيفي، والتخصص)، وتبين عدم وجود فروق ذات دلالة إحصائية عند مستوى الدلالة($0.05\geq\alpha$) بين المتوسطات الحسابية لتقديرات العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية حول الصعوبات التي تواجههم تعزى لمتغير الخبرة، ونوع الجامعة، والمستوى الوظيفي، أما بالنسبة لمتغير الخبرة فهي نتيجة غير متوقعة، إذ يفترض

أن العاملين ذوي الخبرة الأكبر أقل إحساسا للصعوبات، وربما تعزى هذه النتيجة إلى أن المكتبات الجامعية تقوم بتوفير الإمكانات نفسها لجميع العاملين مما يجعل تقديراتهم للصعوبات متقاربة.

وأما بالنسبة لمتغيرات نوع الجامعة والمستوى الوظيفي فهي نتيجة متوقعة لأن المكتبات الجامعية الحكومية والخاصة جميعها متشابهة من حيث التنظيم والخدمات المتوفرة وطبيعة العمل، فالإداريون والموظفون يتعرضون لنفس الظروف ما جعل هناك تقاربا في وجهات النظر.

وكما أظهرت نتائج الجدول رقم (18) وجود فروق أظهرت النتائج كذلك وجود فروق ذات دلالة إحصائية تبعاً لمتغير (التخصص) في (الصعوبات التي تواجه العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية)، واتضح من النتائج أن مصدر الفروق في الصعوبات كان لصالح العاملين في مكتبات الجامعات الأردنية من فئة التخصصات الأخرى ومن ثم لصالح فئة تخصص المكتبات والمعلومات من أفراد مجتمع الدراسة. أي أن متخصصي علم الحاسوب هم أقل إحساسا بالصعوبات، ومن ثم علم المكتبات والمعلومات ثم التخصصات الأخرى. وهي نتيجة متوقعة لأن متخصصي علم الحاسوب هم أقدر على فهم الأمور التقنية. وتتفق هذه النتيجة إلى حد كبير مع دراسة فيليبس PHELPS (2005) التي أشارت إلى أن المكتبيين ذوي التدريب السابق في تكنولوجيا المعلومات كانوا أكثر فعالية في تطبيق أمن نظام المعلومات مقارنة بمن لم يحصلوا على التدريب.

التوصيات:

في ضوء نتائج الدراسة يوصي الباحث بما يلي:

- العمل على مشاركة العاملين بدوائر المعلومات في المكتبات الجامعية في عملية صنع القرار في هذه المكتبات من خلال مناقشة مشكلات العمل وإيجاد رؤية مشتركة فيما يتعلق بأمن المعلومات.
- رفع مستوى البنية التحتية في مكتبات الجامعات الأردنية الحكومية والخاصة وخصوصا الأمن المادي والاهتمام بالبرمجيات المستخدمة وتحديد مسؤوليات الموظفين تجاه أمن المعلومات.
- ضرورة الاهتمام ببناء سياسة واضحة ومكتوبة تتضمن جميع الإجراءات اللازمة لرفع مستوى أمن المعلومات في مكتبات الجامعات الأردنية وضرورة تطويرها كلما تطلب ذلك.
- ضرورة الاهتمام في خدمات النسخ الاحتياطي في المكتبات الجامعية ومتابعتها وتنظيمها وذلك لرفع مستوى حماية البيانات الإلكترونية في مكتبات الجامعات الأردنية.
- المشاركة في المؤتمرات والندوات الداخلية والخارجية للتعرف إلى أهم الطرق والوسائل المستخدمة لرفع مستوى أمن المعلومات في مكتبات الجامعات الأردنية وخفض مستوى الصعوبات في هذا المجال.
- زيادة الكوادر البشرية المتخصصة في أمن المعلومات وعقد الدورات التدريبية للموظفين المتخصصين في أمن المعلومات في مكتبات الجامعات الأردنية وتوفير جميع الإمكانات التي تمكنهم من ذلك.
- وضع أسس موضوعية عند اختيار العاملين بالمكتبات عموما ودوائر المعلومات خصوصا مع مراعاة التخصص، فتمتع هؤلاء العاملين بالكفاءة العالية يمنحهم القدرة على تطبيق معايير أمن المعلومات في مكتبات الجامعات الأردنية.
- ضرورة تطوير المناهج الدراسية في علم المكتبات والمعلومات في الجامعات الأردنية لتشمل مواد دراسية في أمن المعلومات، وبذلك يتم إعداد كوادر بشرية متخصصة في المكتبات قادرة على تطبيق أمن المعلومات فيها.
- العمل على إجراء العديد من الدراسات ذات العلاقة بموضوع الدراسة، لا بل البحث في متغيرات أخرى لها علاقة بأمن المعلومات في مكتبات الجامعات الأردنية، مثل الإدارة، والتخطيط، والإجراءات التي ترفع من مستوى أداء مكتبات الجامعات الأردنية.

المصادر والمراجع

أولاً: المراجع العربية:

أحمد، عوض وخلف، أمير (2002)، **أمنية نظم التشغيل والشبكات الموزعة**، الخرطوم: مطبعة جامعة النيلين.

أكاديمية الفيصل التعليمية (2008)، **أساسيات تكنولوجيا المعلومات**، عمان: زمزم ناشرون.

إبراهيم، السعيد مبروك (2012)، إدارة **المكتبات الجامعية في ضوء اتجاهات الإدارة المعاصرة،** القاهرة: المجموعة العربية.

إبراهيم، السعيد مبروك (2009)، **المكتبة الجامعية وتحديات مجتمع المعلومات**، الإسكندرية: دار الوفاء.

با مفلح، فاتن سعيد (2003)، حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى: دراسة حالة، **مؤتمر الاتحاد العربي للمكتبات والمعلومات الثاني عشر**، المجلد الثاني، جامعة الشارقة، الشارقة، ص.555-590.

بانكس، مايكل (2001)، **أمن الكمبيوتر**، بيروت: الدار العربية للعلوم.

البداينة، ذياب (2002)، **الأمن وحرب المعلومات**، عمان: دار الشروق.

بو عزة، عبدالمجيد صالح (2006)، **المكتبات الرقمية: تحديات الحاضر وآفاق المستقبل،** الرياض: مكتبة الملك فهد الوطنية.

الجواد، دلال والفتال، حميد (2008)، **أمن المعلومات**، عمان: دار اليازوري .

حجار، فادي (2003)، **تشريح الفيروسات**، القاهرة: شعاع للنشر والعلوم.

الخثعمي، مسفرة بنت دخيل الله (2010)، مدى استخدام مصادر المعلومات الإلكترونية: دراسة حالة لأعضاء هيئة التدريس بكلية علوم الحاسب والمعلومات في جامعة الإمام محمد بن سعود الإسلامية بمدينة الرياض. **مجلة مكتبة الملك فهد الوطنية.** 16 (1): 113-130.

خطاب، عامر محمد (2006**)، أمن ومداولات شبكة الإنترنت،** عمان: مكتبة المجتمع العربي.

داود، حسن طاهر (2000)، **الحاسب وأمن المعلومات،** الرياض: مكتبة الملك فهد.

داود، حسن طاهر (2004)، **أمن شبكات المعلومات،** الرياض: مكتبة الملك فهد.

الدباس، ريا أحمد (2010)، **خدمات المعلومات في المكتبات التقليدية والإلكترونية**. عمان: دار البداية.

الدنف، أيمن محمد (2013)، **واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها**. رسالة ماجستير غير منشورة، الجامعة الإسلامية، غزة، فلسطين.

رمضان، علي رشيد (2009)، **أمن المعلومات ونظمها،** فلسطين الخليل: رابطة الجامعيين جامعة بوليتكنك فلسطين.

الزهيمي، صالح (2010)، واقع أمن نظم المعلومات في المكتبات العمانية: دراسة حالة على المكتبة الرئيسية بجامعة السلطان قابوس، **المؤتمر السادس لجمعية المكتبات والمعلومات السعودية**.

السالم، سالم بن محمد (2008)، تطوير العنصر البشري في مجال المكتبات والمعلومات، **مجلة دراسات المعلومات** (3).

السالم، سالم (2009)، السرقات العلمية قضية تهدد أمن المعلومات. **دراسات المعلومات** ، (6)، 5-6.

السالم، سالم (2010). تطوير المهارات التقنية للعاملين في مؤسسات المعلومات، **دراسات المعلومات**، (8).

السرحان، سرحان والمشهداني، محمود (2001)، **أمن الحاسوب والمعلومات،** عمان: دار وائل.

السريحي، حسن (2002)، أمن المكتبات ونظم المعلومات دراسة حالة على مكتبة جامعة الملك عبد العزيز بجدة. **مجلة مكتبة الملك فهد الوطنية**. 8 (1)، 112-154.

سلامة، محمد عبد الله (2006)، **جرائم الكمبيوتر والإنترنت**، الإسكندرية: منشأة المعارف.

الشوابكة، يونس (2010)، استخدام مصادر المعلومات الإلكترونية المعتمدة على الإنترنت في الرسائل والأطروحات الجامعية التربوية: دراسة تحليلية للاستشهادات المرجعية، **المجلة الأردنية في العلوم التربوية**، 6 (4): 303-317.

الصاحب، محمود حسن (2013)، سياسة أمن المعلومات في الجامعات: حالة دراسية. **Cybrarian Journal**. (33).

الصلاح، تحسين محمد (2006)، **مكتبة الجامعة الأردنية تاريخ وتطور**، عمان: مكتبة الجامعة الأردنية.

الطائي، محمد عبد المحسن والكيلاني، ينال محمود (2015)، **إدارة أمن المعلومات**، عمان: دار الثقافة.

الطيطي، خضر مصباح (2010)، **أساسيات أمن المعلومات والحاسوب**، عمان: دار الحامد للنشر والتوزيع.

عرب، يونس (2005). أمن المعلومات ماهيتها وعناصرها وإستراتيجياتها، تاريخ الاطلاع 2016/5/15. متاح في:

http://www.dralmarri.com/show.asp?field=res_a&id=205

العربي، أحمد عيادة، (2013)، المعايير الدولية لسياسات أمن المعلومات: دراسة تحليلية لمعايير المنظمة الدولية للتوحيد القياسي(آيزو2700002 ISO/IEEC) ومدى تطبيقها في الجامعات العربية، **مجلة مكتبة الملك فهد**، 19 (2).

علوة، رأفت نبيل (2011)، **قرصنة الإنترنت**، عمان: مكتبة المجتمع العربي.

عليان، ربحي وأبو زيد، محمد (2002). ضغوط العمل لدى العاملين في المكتبات الجامعية الحكومية والخاصة في الأردن، **مجلة دراسات**، الجامعة الأردنية، 2(29)، 334-350.

عليان، ربحي مصطفى، (2010)، **المكتبات الإلكترونية والمكتبات الرقمية**، عمان:دار صفاء.

عليان، ربحي مصطفى، (2014)،**المكتبات المتخصصة ومراكز المعلومات**، عمان: دار صفاء.

عليوي، محمد والمالكي، مجبل، (2007)، **المكتبات النوعية**، عمان: الوراق.

عمار، زكريا أحمد، (2011)، **حماية الشبكات الرئيسية من الاختراق والبرامج الضارة، رسالة** ماجستير غير منشورة، جامعة النيلين، الخرطوم، السودان.

الغثبر، خالد بن سليمان والصبيح، أمل ناصر (2012)، حال أمن المعلومات في المملكة العربية السعودية، **دراسات المعلومات**، (14): 189-205.

الغثبر، خالد بن سليمان والقحطاني، محمد بن عبد الله (2009)، **أمن المعلومات**، الرياض: مركز التميز لأمن المعلومات.

القحطاني، ذيب (2008)، **المدخل إلى أمن المعلومات**، الرياض: مكتبة الملك فهد.

الكردي، أحمد (2011)، سياسة أمن المعلومات، منتدى كنانة، تاريخ الدخول 2016/5/19 متوفر على الموقع الإلكتروني:

http://kenanaonline.com/users/ahmedkordy/posts/320944

الكردي، أحمد (2011)، إستراتيجيات النسخ الاحتياطي، منتدى كنانة، تاريخ الدخول 2016/5/15، متوفر على الموقع الإلكتروني:

http://kenanaonline.com/users/ahmedkordy/posts/320934

اللوزي، موسى سلامة (2010)، الصعوبات التي تواجه تطبيق الخدمات الاإكترونية كما يراها العاملون في أجهزة الخدمة المدنية في الأردن، **المجلة الأردنية في إدارة الأعمال**،6 (1).

المصري، أحمد طلبة (2015)، **قواعد البيانات في المكتبات والمعلومات**، عمان: الوراق.

المصري، عبد الصبور (2008)، **الجريمة الإلكترونية**، القاهرة: دار العلوم.

مكتبة الجامعة الأردنية، استرجع بتاريخ 2016/5/20 من:

http:// library.ju.edu.jo

ملحم، عصام توفيق (2011)، **مصادر المعلومات الإلكترونية في المكتبات الجامعية**، الرياض: جامعة نايف العربية للعلوم الأمنية.

موسى، غادة عبد المنعم (2012)، **مكتبات المؤسسات التعليمية: ماهيتها، مقوماتها، خدماتها، تسويقها**، الاسكندرية: دار المعرفة الجامعية.

النوايسة، غالب عوض (2011)، **مصادر المعلومات لإلكترونية في المكتبات ومراكز المعلومات**، عمان: دار صفاء.

الهادي، محمد (2006)، توجهات أمن وشفافية المعلومات في ظل الحكومة الإلكترونية، **مجلة Cybrarians journal**، (9).

همشري، عمر أحمد (2009)، **المكتبة ومهارات استخدامها**، عمان: دار صفاء.

يونس، عبد الرازق (2003)، أثر استخدام النظم الآلية على إدارة المكتبات الجامعية في الأردن، **مجلة جامعة الملك سعود**، 16 (1): 197-233.

ثانياً: المراجع الأجنبية:

Akor, Phlip Usman (2013), Security Management For Prevention of Book Thefts in University Libraries.A Case Study of Benue State University Library, Nigeria, **Library Philosophy and Practice (e-journal)**.995.

Braker, Wade and Wallace, linda. (2007), Is Information Security Under Control: Investigating Quality in Information Security Management, **IEE Security and Privacy**.5 (1): 36-44.

Bugurcu, Brcu. Cavusoglu, Hasan and Bendbasat, Izak. (2010), Information Security Policy Complaiance: An Empirical Study of Rationality-Based Belifs and Information Security Awareness, **MIS Quarterely**. 34 (3): 524-548.

Eloff,h and Eloff, Mariki. (2003), Information Security Management: a new Paradigm.**Conference of Enablement Through Technology**, 47: 130-136.

Fulfurd, H and Doherty,n f. (2003), The Application of Information Security Policies in Large UK-based Organizations: an exploratory Investigation. **Information Management and Computer security**, 11 (3): 106-114.

Ismail, Roesnita& Awang, Zainab (2011), Information systems security inspecial and public libraries: an Assessment of Status, **Malaysian Journal of Library & Information Science**, 16(2): 45-62.

Ismail, Roesnita (2012), **Assessing Information Security Management in Malasian Academic Libraries.** Unpublished Doctoral Dissertation, University of Malaya, Kuala Lumpur.

Jain,Anil. Ross,Aron and Pankanti,Sharath. (2006), Biometrics: A Tool for Information Security. **IEEE Transacions Forensics and Security**, 1 (2):125-143.

Kankanhalli, Atereyi. Teo, Hok Hai. Tan, Bernard and Wei, Kowok. (2003).an integrative study of information systems swcurity effectiveness. **International Journal Information Management**, (23): 139-154.

Knapp,Kennth. Jr, R Franklin. Marsall, Thomas and Byrd, Terry. (2009), Information Security Policy: An Organizational- Level Process Model,**Computer& Security**, 28 (7): 493-508.

Kritzinger,E and Smith, E. (2008). Information Security Management: AN Information Security Retrieval and Awareness Model for Industry, **Computers and Security**, 27 (5): 224- 231.

Maidabino, Abass & Awang, Zainab (2011), Collection Security Management at University Libraries: Assesment of its Implementation Status. **Malaysian Journal of Library & Information Science**, 16(1): 15-33.

Newby, Gregory B. (2002), Information Security for Libraries. **Modern Organization in Virtual Communities**: 134-144.

Osyande, Odaro, (2011), Electronic Security Systems in Academic libraries: A Case Study of Three University Libraries in South-West Nigeria, **Chinese Librarianship: an International Electronic Journal**, 32: 1-10.

Phelps, Daniel C, (2005), **Information System Security: SELF-Efficacy And Security Effectiveness In Florida Libraries.** Unpublished Doctoral Dissertation, The Florida State University, Florida,USA.

Roberto, jose and Araujo, Vaessa. (2009). A modified Epidemiological Model for Computer Viruses. **Applied Mathematics and Computation**, 213: 355-360.

Shaw,R S. Charlie, C Chen. Albert L Harris and Hui Jou Huang. (2009), The Impact of Information Richness on Information Security

Awareness Training Effectiveness. **Computers and Education**, 52 (1): 92-100.

Sirma, Jerotich and Kipchillat, Cynthia. (2014). Impact of Information Security Policies on Computer Security Breach Incidences in Kenyan Public Universities. **Information and Knowledge Management**, 14 (9):42-50.

Summer,Mary. (2009), Information Security Threats: A Comparative of Impact, probability,and Preparedness. **Information Systems Management**, 26 (1): 2-12.

Whitman, Michael. (2004), In Defense of the Realm: Understanding the threats to Information Security. **International Journal Information Management**, (24): 43-57.

الملحق رقم (1)

أداة الدراسة (الاستبانة)

بسم الله الرحمن الرحيم

الزميل/ة المحترم/ة

السلام عليكم ورحمة الله وبركاته

يقوم الباحث بإعداد رسالة ماجستير بعنوان " **أمن المعلومات من وجهة نظر العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية والصعوبات التي يواجهونها**"، وذلك استكمالاً لمتطلبات الحصول على درجة الماجستير في علم المكتبات والمعلومات من الجامعة الأردنية، وسيشمل مجتمع الدراسة العاملين بدوائر المعلومات في مكتبات الجامعات الأردنية، لذا أرجو التكرم من سيادتكم بقراءة كل فقرة من فقرات الاستبانة ووضع علامة (√) في الخانة التي تمثل وجهة نظركم وفق تدرج خماسي (موافق بشدة، موافق، محايد، غير موافق، غير موافق بشدة). علما بأن إجابتكم ستستخدم لأغراض البحث العلمي فقط.

ولكم خالص تحياتي وجزيل الشكر

الباحث

حسام المصالحه

أولاً: المعلومات الشخصية:

يرجى وضع إشارة (√) في المربع المناسب:

الخبرة: ☐ 5 سنوات فما دون . ☐ 6-10 سنوات.
☐ أكثر من 11.

نوع الجامعة: ☐ حكومية. ☐ خاصة.

المستوى الوظيفي : ☐ مدير . ☐ رئيس قسم / شعبة . ☐ موظف.

التخصص: ☐ هندسة حاسوب. ☐ مكتبات ومعلومات.
☐ علم الحاسوب ☐ تخصص آخر.

ثانياً: محاور الدراسة

المحور الأول: أمن البنية التحتية في المكتبات

أ. الأمن المادي

الرقم	العبارة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
1	يوجد مصدر احتياطي للكهرباء داخل المكتبة.					
2	جميع كوابل الكهرباء والاتصالات التي تنقل البيانات محمية من العبث بها أو الإتلاف داخل المكتبة.					
3	يتوافر وسائل تصريف للمياه ومضخات شفط عند الحاجة.					
4	يتوافر أجهزة لكشف الحريق والإنذار حالة حدوثه.					
5	مداخل ومخارج المكتبة مؤمنة بأجهزة إنذار إلكترونية.					
6	يتوافر بالمكتبة أجهزة تكييف وتهوية كافية.					
7	هناك صيانة مستمرة للأجهزة بشكل يضمن استمرارية عملها.					
8	يمنع الموظف غير المختص من إجراء أي تعديل مادي على الأجهزة في المكتبة.					

ب. حماية الأفراد

الرقم	العبارة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
9	يتم متابعة المستخدمين وتسجيل الحوادث التي تخص أمن المعلومات داخل المكتبة .					
10	يتم تحديد مسؤوليات الموظف ومهماته تجاه أمن المعلومات في المكتبة.					
11	يشترط على الموظفين عدم إفشاء اجراءات الأمن والرقابة.					

12	يتم محاسبة الموظف الذي ينتهك اجراءات أمن المعلومات داخل المكتبة.					

ج. أمن البرمجية

الرقم	العبارة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
13	يتم التحقق من صحة البيانات المدخلة.					
14	يتم استخدام آليات تشفير لحماية البيانات.					
15	تتوافر تعليمات تضمن إجراء عملية التشفير بطريقة آمنة.					
16	تتوافر معايير لقبول أي نظم جديدة أو تعديل وإجراء اختبارات عليها قبل القبول بها.					
17	يتم حماية النظام عن طريق برامج مكافحة الفيروسات.					
18	يتوفر برامج لتتبع الاختراق والتسلل.					
19	جميع برامج مكافحة الفيروسات والاختراق والتسلل موثوقة ومرخصة.					
20	يتم تحديث برامج مكافحة الفيروسات والاختراق والتسلل بشكل مستمر.					

المحور الثاني: سياسة أمن المعلومات

الرقم	العبارة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
21	يتوفر في المكتبة سياسة مكتوبة ومعتمدة لأمن المعلومات.					
22	تحدد هذه السياسة المسؤوليات والصلاحيات مثل صلاحية منع المستخدم من الدخول للشبكة.					
23	تتضمن هذه السياسة إجراءات الوقاية من المخاطر.					
24	تتضمن هذه السياسة أمن الإجراءات التي يجب اتباعها عند ظهور المشاكل.					
25	يتم مناقشة وتطوير سياسة أمن المعلومات بشكل دوري.					

المحور الثالث: حماية البيانات الإلكترونية في المكتبة

الرقم	العبارة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
26	يتوافر في المكتبة خدمة النسخ الاحتياطي لحماية البيانات الموجودة على الحاسوب.					
27	يتم متابعة عملية النسخ الاحتياطي للتأكد من أنها تتم بالشكل الصحيح.					
28	عندما تكون المعلومات المخزنة على وسائل النسخ الاحتياطي سرية يتم تشفيرها حسب السياسة المتبعة لذلك.					
29	يتم تصنيف النسخ الاحتياطي حسب الفترة الزمنية التي تتم بها عملية النسخ لتسهيل الرجوع إليها.					
30	يتم تخزين وسائط البيانات الإلكترونية في أماكن خارجية آمنة.					
31	يتم إتلاف وسائط التخزين الاحتياطي بطريقة آمنة عند إعادة استخدامها.					

المحور الرابع: إجراءات حماية أنظمة وشبكات الحاسوب في المكتبة.

الرقم	العبارة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
32	يتم تحديث نظم التشغيل في حال توجب ذلك (اختراق، خلل في عناصر الحماية الخاصة).					
33	يتم وضع كلمات مرور للدخول إلى الشبكة تعطى للأشخاص المخولين.					
34	يتوافر أجهزة تدعم حماية الشبكة الداخلية مثل أنظمة كشف ومنع الاختراق والجدران النارية fir wall وغيرها.					
35	يتم ضبط الاعدادات الخاصة بالأجهزة الموجودة على الشبكات لتعمل بطريقة آمنة.					
36	يتم رفع تقارير دورية توضح المشاكل الأمنية التي تمت مواجهتها على الشبكة.					

37	يتم أخذ الموافقة قبل التعديل على الأجهزة وبرامج الحماية.					
38	تحتفظ المكتبة بسجلات حول الأصول المكونة لكل نظام معلومات.					
39	في حال وجود إخفاق أو انقطاع في أداء الأعمال توجد خطة لإعادة الأعمال إلى طبيعتها ضمن إطار زمني مخطط.					
40	يتم تسجيل ما يحدث من أخطاء في نظم المعلومات في تقارير ويتم توثيق الإجراءات التي اتخذت لتصحيحها.					

المحور الخامس: التحكم بالوصول لنظم المعلومات

الرقم	العبارة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
41	يتم إعطاء مجموعة من الصلاحيات لكل مستخدم حسب المستوى الإداري.					
42	يتم إعطاء كل مستخدم هوية خاصة به حيث لا يوجد صلاحيات عامة يستخدمها عدة أشخاص					
43	يتم إغلاق صلاحيات المستخدم لدواع متعلقة بأمن المعلومات.					
44	توجد مراجعات دورية لصلاحيات المستخدمين في الوصول للمعلومات.					
45	يتم تسجيل العملية التي يقوم بها المستفيد بعد تنفيذها.					
46	هناك تقارير عن الأنشطة التي يقوم بها المستخدم.					
47	تتوافر إرشادات لطريقة إنشاء كلمات مرور فورية.					
48	بعض أنظمة المعلومات الحساسة معزولة في شبكات محلية مستقلة.					
49	تستخدم سجلات الأداء لحفظ أنشطة المستخدم لدواعي متعلقة بأمن المعلومات.					

ثالثاً: الرجاء بالتفضل بإبداء رأيكم حول الصعوبات التي تواجه العاملين بدوائر المعلومات في المكتبة التي تعملون بها.

الرقم	العبارة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
50	هناك نقص في الموازنة المخصصة لأمن المعلومات في المكتبة.					
51	هناك صعوبة في توفير برامج لحماية أمن المعلومات الفعالة.					
52	نقص الموظفين المتخصصين في أمن المعلومات					
53	هناك تزايد في إمكانية التعرض لمخاطر أمن المعلومات .					
54	صعوبة مواكبة الابتكارات والأساليب الحديثة في مجال أمن المعلومات.					
55	لا تتوافر الأدوات اللازمة التي تمكن المختصين بأمن المعلومات من تطوير عملهم.					
56	هناك صعوبات في تحديد حجم الخسارة الناجمة عن مختلف حوادث الانتهاك أحيانا.					
57	يوجد صعوبات في تحديد كفاية الإجراءات الأمنية الحالية أو عدم كفايتها.					
58	قلة الوقت الكافي لمناقشة الطرق الجديدة لحماية أمن المعلومات.					
59	ضعف الاهتمام من قبل الادارة في الملاحظات التي رصدت.					
60	ضعف التدريب على المهارات المطلوبة في مجال أمن المعلومات.					

الملحق رقم (2)

قائمة بأسماء المحكمين

الرقم	الاسم	الجامعة التي يعمل بها	القسم
1	الأستاذ الدكتور عبد الرازق يونس	الجامعة الأردنية	علم المكتبات والمعلومات
2	الأستاذ الدكتور ربحي مصطفى عليان	الجامعة الأردنية	علم المكتبات والمعلومات
3	الدكتور يونس أحمد الشوابكه	الجامعة الأردنية	علم المكتبات والمعلومات
4	الدكتورة فاتن حمد	الجامعة الأردنية	علم المكتبات والمعلومات
5	الدكتورة دينا طبيشات	الجامعة الأردنية	علم المكتبات والمعلومات
6	الدكتور رائد جميل	الجامعة الأردنية	علم المكتبات والمعلومات
7	الدكتور رزق محمد السيد	الجامعة الأردنية	تكنولوجيا معلومات الأعمال
8	الدكتور حسام عمر فارس	الجامعة الأردنية	تكنولوجيا معلومات الأعمال
9	الدكتور يزن ياسين الشمايلة	الجامعة الأردنية	تكنولوجيا معلومات الأعمال
10	الدكتور أسامة محمد ربابعة	الجامعة الأردنية	تكنولوجيا معلومات الأعمال
11	الدكتور عبداللطيف أبو دلهوم	الجامعة الأردنية	علم الحاسوب
12	الدكتور ساهر المناصير	الجامعة الأردنية	علم الحاسوب
13	الدكتور نزار راسم اللبدي	الجامعة الأردنية	علم النفس التربوي

THE STATUS QUO OF INFORMATION SECURITY FROM THE PERSPECTIVE OF EMPLOYEE IN THE INFORMATION UNITS IN THE JORDANIAN UNIVERSITY LIBRARIES AND DIFFICUITIES THEY FACE

BY
Hussam Mohammed Fahd Almasalha

Supervisor
Dr. Nashrawan Taha

ABSTRACT

This study aimed at exploring the status quo of information security from the perspective of the employee in the information units in Jordanian university libraries. Furthermore, it looked at the main difficulties they would face. The study also aimed at studying the effect of some variables related to those employee; namely :years of experience, the type of university, functional level, and their specialization on the status quo of information security, and the difficulties they were facing.

The study population consisted of all libraries employees in the Jordanian public and private universities for the academic year 2015-2016, where the sample of the study consisted of 96 employees, of whom 84 has responded, with 87.5% rate. A questionnaire was developed which consisted of five areas: security of infrastructure, information security policies, protection electronic data, computer networks and procedures of systems protection and access control of information systems. The questionnaire has also included questions about the difficulties that could face the employee in information units.

The research findings showed that the status quo of information security in the Jordanian university libraries from the perspective of employee in information units was average, where the paragraph related to protecting computer networks and information systems, and control access to information systems have scored a high score. The other paragraphs have scored average score. In regards to the difficulties that faced the employee working in information units at university libraries, it has received an average level, where the findings showed that the main difficulty they were facing was the lack of specialists' staff in information security.

The study showed a significant difference at ($\alpha \leq 0.05$) in the status quo of information security related to the variables of the functional level and specialization. However, there was no significant difference related to the other variables; years of experience and the type of university. Furthermore, the differences in the difficulties facing employee working in information units have shown a significant difference in the difficulties they face related to the variable of specialization, while the other variables; years of experience, university type- have shown no statistical difference.